

**THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re the Application of : Katsuichi NAKAMURA, et al.

Filed : Concurrently herewith

For : NETWORK ACCESS CONTROL METHOD,.....

Serial No. : Concurrently herewith

March 26, 2001

Assistant Commissioner of Patents  
Washington, D.C. 20231

**SUBMISSION OF PRIORITY DOCUMENT**

S I R:

Attached herewith are Japanese patent application No.  
2000-331345 of October 30, 2000 whose priority has been claimed  
in the present application.

Respectfully submitted



[ ] Samson Helfgott

Reg. No. 23,072

[x] Aaron B. Karas

Reg. No. 18,923

HELFGOTT & KARAS, P.C.  
60th FLOOR  
EMPIRE STATE BUILDING  
NEW YORK, NY 10118  
DOCKET NO.: FUJI 18.503  
BHU:priority

Filed Via Express Mail

Rec. No.: EL522402486US

On: March 26, 2001

By: Brendy Lynn Belony

Any fee due as a result of this paper,  
not covered by an enclosed check may be  
charged on Deposit Acct. No. 08-1634.

#2  
JCS97 U.S. PTO  
09/017303  
03/26/01

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

#2

JC997 U.S. PTO  
09/817303



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

2000年10月30日

出願番号  
Application Number:

特願2000-331345

出願人  
Applicant(s):

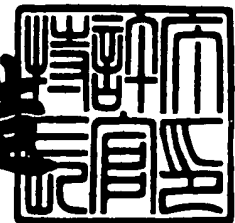
富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 2月23日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2001-3011258

【書類名】 特許願

【整理番号】 0051762

【提出日】 平成12年10月30日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 H04L 12/40

【発明の名称】 ネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置

【請求項の数】 5

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

【氏名】 中村 勝一

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

【氏名】 山村 新也

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜2丁目2番1号 富士通西日本コミュニケーション・システムズ株式会社内

【氏名】 佐藤 義治

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100070150

【住所又は居所】 東京都渋谷区恵比寿4丁目20番3号 恵比寿ガーデンプレイスタワー32階

【弁理士】

【氏名又は名称】 伊東 忠彦

【電話番号】 03-5424-2511

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704678

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置

【特許請求の範囲】

【請求項 1】 パケットフィルタリング機能を有するネットワーク装置と、  
前記ネットワーク装置を介して I P ネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介して I P ネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記 I P ネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付ける受付サーバと、

前記ネットワーク装置を制御するアクセス制御サーバと、で構成されるネットワークシステムのネットワークアクセス制御方法において、

前記受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うことを特徴とするネットワークアクセス制御方法。

【請求項 2】 パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介して I P ネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介して I P ネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記 I P ネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付けるアクセス受付手段を備えた受付サーバと、

前記ネットワーク装置を制御するトラヒック制御手段を備えたアクセス制御サーバと、で構成されるネットワークシステムにおいて、

前記受付サーバは、前記アクセス受付手段を介しユーザ端末からのアクセス要

求情報を受信して保持するアクセス登録手段を有し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラフィック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラフィック制御を行うフィルタリング最適化手段を有することを特徴とするネットワークシステム。

【請求項 3】 ユーザ端末からのアクセス要求情報を保持するアクセスリストと、

各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロフィールと、  
ユーザ端末からのアクセスを受け付けるアクセス受付手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリストに受付順に登録するアクセス登録手段と、

受信したアクセス要求情報から IP アドレスを抽出し、IP アドレスによりユーザを特定して前記ユーザプロフィールからユーザクラスを抽出するユーザクラス抽出手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザクラス別アクセス登録手段を

有することを特徴とする受付サーバ。

【請求項 4】 請求項 3 記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位置に応じた待ち合わせを行っているユーザ数から予測待ち合わせ時間を算出する予測待合時間算出手段と、

算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を有することを特徴とする受付サーバ。

【請求項 5】 請求項 3 記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するア

クセス確認手段と、

前記アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を有することを特徴とする受付サーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置に関し、特に、IPネットワークのネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置に関する。

【0002】

【従来の技術】

従来のネットワークアクセス制御方法として、プロキシ・サーバによるアクセス制限方法がある。プロキシ・サーバとは、マルチメディア・データベース、WWW (World Wide Web) など、インターネットの様々なサービスへのアクセスを中継するためのソフトウェア、またはサーバ・マシンである。

【0003】

プロキシ・サーバは、社内ネットワークとインターネット間のトラフィックを軽減したい時などキャッシュ機能として使用する。例えば、社内のユーザーがあるWWWのページのアクセスすると、その内容をプロキシサーバは一定期間記憶しておく。次に別のユーザーが同じページにアクセスした場合は、インターネットにアクセスする必要はなく、プロキシサーバが持つ情報をユーザーに返送する。このようにしてインターネット・アクセスの頻度を減らせる。

【0004】

また、サーバアプリケーションで、接続コネクション数を予め設定するアクセス制限方法がある。例えば特開平5-316115公報に記載のものは、複数の端末を接続するコンピュータネットワークを複数相互接続し、日付・曜日・時間あるいはグループ番号等によるアクセス制御をすることで、専用回線の負荷分散

を効率よく正確に行えることを目的とし、予め設定した情報テーブル（日付・曜日・時間、グループ番号からなる）を参照し、ネットワークのアクセス制御を行う。

#### 【0005】

また、特開平6-152615公報に記載のように、複数伝送路の効率的な均等負荷制御を行うことを目的とし、伝送路の負荷計測機能と伝送路切替え制御機能を具備して、伝送路対応の負荷（トラフィック量）を計測して負荷の低い経路を選択することを特徴とするネットワークアクセス制御方法がある。

#### 【0006】

更に、トラフィックが集中するサーバに対する負荷分散を目的とし、複数のミラーサーバを設け、サーバとミラーサーバの負荷状況を計測しミラーサーバから最も負荷の低いサーバにアクセスさせるという負荷バランスシステムも提案されている。

#### 【0007】

##### 【発明が解決しようとする課題】

プロキシ・サーバを使用した方法では、コンテンツ・オブジェクトが一度キャッシュに蓄えられた後、情報発信元のオブジェクトが更新された場合、2回目以降はオブジェクトの実体にアクセスしないのでオブジェクトが更新されず、何回リクエストしても新しい情報が入手できないことになる。さらに、サーチエンジンの検索結果でアクセスする度に内容が変化する（カウンタなど）動的なオブジェクトは再利用できない。また、キャッシュ機能にもメモリ容量やディスク容量の制限があるため、有効と思われるオブジェクトでも状況によって消去しなければならないという問題がある。

#### 【0008】

接続コネクション数を予め設定する方法は、トラフィック集中時に利用者は何度もアクセスしないとならないので、無意味なトラフィックがネットワーク上を流れる事になる。更に、予め設定した情報（日付・曜日・時間）によって、またはトラフィック量を計測することによって負荷の低い経路を選択した場合でも、接続先のサーバがそれに耐えられる処理能力を持たないと最適な経路選択は効果を十分



生かせないという問題がある。

【 0 0 0 9 】

また、サーバとミラーサーバの負荷状況を計測し負荷の低いサーバにアクセスさせる方法は、利用者からのアクセスを割り振っただけなので、サーバやミラーサーバ毎に発生する高負荷の場合のアクセス制御は行われない。トラヒックが集中するサーバに対しては、ネットワーク側でもアクセス規制を行わないとミラーサーバを無意味に増やすだけになるという問題がある。

【 0 0 1 0 】

本発明は、上記の点に鑑みなされたものであり、動的オブジェクトを再利用でき、トラヒックの軽減を図ることができ、ユーザに与える負担を軽減でき、アクセス要求したユーザは自分のアクセス順番になれば速い応答速度で快適にサービスを受けることが可能となるネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置を提供することを目的とする。

【 0 0 1 1 】

【課題を解決するための手段】

請求項 1 に記載の発明は、パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介して IP ネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介して IP ネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記 IP ネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付ける受付サーバと、

前記ネットワーク装置を制御するアクセス制御サーバと、で構成されるネットワークシステムのネットワークアクセス制御方法において、

前記受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアク

セスを許容するトラヒック制御を行うため、

ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

#### 【 0 0 1 2 】

請求項 2 に記載の発明は、パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介して I P ネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介して I P ネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記 I P ネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付けるアクセス受付手段を備えた受付サーバと、

前記ネットワーク装置を制御するトラヒック制御手段を備えたアクセス制御サーバと、で構成されるネットワークシステムにおいて、

前記受付サーバは、前記アクセス受付手段を介しユーザ端末からのアクセス要求情報を受信して保持するアクセス登録手段を有し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うフィルタリング最適化手段を有するため、

ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

#### 【 0 0 1 3 】

請求項 3 に記載の発明は、ユーザ端末からのアクセス要求情報を保持するアクセスリストと、

各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロフィールと、  
ユーザ端末からのアクセスを受け付けるアクセス受付手段と、  
前記アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリスト  
に受付順に登録するアクセス登録手段と、

受信したアクセス要求情報から I P アドレスを抽出し、 I P アドレスによりユー  
ーザを特定して前記ユーザプロフィールからユーザクラスを抽出するユーザクラ  
ス抽出手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽  
出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザ  
クラス別アクセス登録手段を有するため、

ユーザクラス別にユーザからのアクセス要求情報を登録することができる。

【 0 0 1 4 】

請求項 4 に記載の発明は、請求項 3 記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位  
置に応じた待ち合わせを行っているユーザ数から予測待ち合わせ時間を算出する  
予測待ち時間算出手段と、

算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過  
後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を有  
するため、

ユーザにサービスへのアクセス可能となるまでの時間を通知してユーザからの  
アクセス要求の待合せを可能とし、ユーザに与える負担を軽減できる。

【 0 0 1 5 】

請求項 5 に記載の発明は、請求項 3 記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、  
前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するア  
クセス確認手段と、

前記アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を有  
するため、

ユーザに待合せを行うことを確認することができる。

## 【 0 0 1 6 】

付記 6 に記載の発明は、サービスサーバの処理能力に関する情報及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持するアクセス情報データベースと、

ネットワーク装置を制御するトラヒック制御手段と、

前記サービスサーバの処理能力に関する情報に基づき最大アクセス許容数を算出する静的アクセス許容数算出手段と、

受付サーバでユーザ端末からのアクセス要求情報を保持するアクセスリストの先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバにアクセス可能とするパケットフィルタリング設定情報を生成し前記トラヒック制御手段を介して前記ネットワーク装置に設定するフィルタリング最適化手段を有するため、

サービスサーバの処理能力に見合うユーザからのアクセスを受け付ける制御を行うことができる。

## 【 0 0 1 7 】

付記 7 に記載の発明は、付記 6 記載のアクセス制御サーバにおいて、

前記サービスサーバの負荷状態及びサービスサーバを収容するネットワーク装置のトラフィック状態を監視する負荷・トラヒック監視装置と、

周期的に負荷・トラヒック監視装置と通信して前記負荷状態及びトラヒック状態の情報を抽出して前記アクセス情報データベースの最大アクセス許容数を算出すると共に、算出した最大アクセス許容数を前記アクセス情報データベースに登録する動的アクセス許容数算出手段を有するため、

サービスサーバの負荷状況やトラヒック状況に応じてサービスサーバが最適に動作可能なアクセス分のユーザにアクセスを許可することが可能となる。

## 【 0 0 1 8 】

付記 8 に記載の発明は、付記 6 記載のアクセス制御サーバにおいて、

ユーザ端末からのアクセス要求情報を前記アクセスリストから読み出す際に読み出す指針となる制御情報を保持する制御情報データベースと、

前記フィルタリング最適化手段が前記アクセスリストから最大アクセス許容数

分のアクセス要求情報を読み出す際に前記アクセスリストがユーザクラス別に登録されている場合、前記制御情報データベースから抽出された制御情報に基づき前記アクセスリストの各ユーザクラスからアクセス要求情報を読み出すユーザクラス別アクセス要求読出手段を有するため、

ユーザクラスに応じて読み出すアクセス要求情報数を可変することができる。

#### 【0019】

付記9に記載の発明は、付記6記載のアクセス制御サーバにおいて、

パケットフィルタリング設定情報を生成する際にアクセス要求情報に有効タイマを設定する有効タイマ設定手段と、

前記有効タイマの満了時にネットワーク装置に設定したパケットフィルタリング制御を解除するフィルタリング解除手段を有するため、

有効タイマを用いて各アクセスの時間管理を行い、アクセス許可を解除することができる。

#### 【0020】

付記10に記載の発明は、ネットワーク装置を介してIPネットワークに接続され、ユーザにサービスを提供するサービスサーバにおいて、

ユーザ端末とのセッションを終了したこと判定するセッション終了判定手段と

前記ユーザ端末とのセッションを終了したことをアクセス制御サーバに通知するセッション終了通知手段を有するため、

セッションが終了したアクセスのアクセス許可を解除することができる。

#### 【0021】

付記11に記載の発明は、請求項3記載の受付サーバにおいて、

前記ユーザクラス抽出手段で抽出したユーザクラスに基づき前記アクセス受付手段を介し受信したアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバにその旨を通知するユーザ認証手段を有し、また、付記12に記載の発明は、付記6記載のアクセス制御サーバにおいて、

付記11記載の受付サーバのユーザ認証手段からの通知に基づき前記サービスサーバにアクセス不許可とするパケットフィルタリング設定情報を生成して前記

ネットワーク装置に設定するアクセス不許可フィルタリング設定手段を有するため、

ユーザがアクセス権限を持っている場合にのみサービスサーバのアクセスを許可することができる。

#### 【発明の実施の形態】

図 1 は、本発明方法の一実施例の全体構成図を示す。同図中、コアネットワーク（IP ネットワーク）10 にはルータ等のネットワーク装置 20, 30, 40 が設けられている。ネットワーク装置 20, 30 はパケットフィルタリング機能を有しており、ネットワーク装置 20 にはユーザ端末 50 が接続され、ネットワーク装置 30 にはユーザにサービスを提供するサービスサーバ 300 が接続されている。

#### 【0022】

また、ネットワーク装置 40 には、サービスサーバ 300 の受付としてユーザからのアクセスを受け付ける受付サーバ 100 と、ネットワーク装置 40 を制御すると共にサービスサーバ 300 の負荷状態やサービスサーバ 300 を収容するネットワーク装置 30 のトラフィック状態を監視するアクセス制御サーバ 200 とが接続されている。

#### 【0023】

受付サーバ 100 において、ユーザプロフィール 111 は、各ユーザのユーザクラス等のユーザ情報を保持する。アクセスリスト 109 は、ユーザからのアクセス要求情報を保持する。アクセス受付手段 110 は、ユーザからのアクセスを受け付ける。アクセス登録手段 103 は、アクセス受付手段 110 を介しユーザからのアクセス要求情報を受信し、このアクセス要求情報をアクセスリスト 109 に受付順に登録する。

#### 【0024】

ユーザクラス抽出手段 102 は、アクセス受付手段 103 を介しユーザからのアクセス要求情報を受信し、このアクセス要求情報から IP アドレスを抽出し、IP アドレスによりユーザを特定し、ユーザプロフィールからユーザクラス抽出する。ユーザクラス別アクセス登録手段 108 は、ユーザクラス抽出手段 102

を介し取得したユーザクラスに基づいて、アクセス要求情報をアクセスリストに登録する。予測待合時間算出手段106は、ユーザからのアクセス要求を受け付けた際に、本アクセス要求をアクセスリスト109に登録する位置から、既存のAI機能及び統計手法等を用いて、予測待ち合わせ時間を算出する。アクセス情報通知手段107は、算出した予測待ち合わせ時間の情報をユーザに通知し、予測待ち合わせ時間経過後、ユーザにアクセス可能であることを通知する。

## 【0025】

アクセス確認手段104は、ユーザからのアクセス要求を受け付けた際に、本アクセス要求をアクセスリスト109に登録するか否かをユーザに確認する。待合せ確認通知手段105は、アクセス要求をアクセスリスト109に登録するか否かをユーザに確認通知する。ユーザ認証手段101は、ユーザクラス抽出手段102を介し取得したユーザクラスに基づいてアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバ200にその旨を通知する。

## 【0026】

アクセス制御サーバ200において、アクセス情報DB（データベース）209は、サービスサーバ300の処理能力に関する情報、及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持する。制御情報DB（データベース）211は、ユーザからのアクセス要求情報をアクセスリスト109から読み出す際に、読み出す指針となる制御情報を保持する。トラヒック制御手段210は、ネットワーク装置40を制御する。負荷・トラヒック監視装置212は、サービスサーバ300の負荷状態やサービスサーバ300を収容するネットワーク装置30のトラフィック状態を監視する。

## 【0027】

静的アクセス許容数算出手段206は、サービスサーバ300の処理能力に関する情報に基づき最大アクセス許容数を算出する。フィルタリング最適化手段204は、アクセスリスト109の先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバ300にアクセス可能とするパケットフィルタリング設定情報を生成し、このパケットフィ

ルタリング設定情報をトラヒック制御手段210を介して、ネットワーク装置20, 30に設定する。動的アクセス許容数算出手段207は、周期的に負荷・トラヒック監視装置212と通信して負荷状態及びトラヒック状態の情報を抽出し、アクセス情報DB209の最大アクセス許容数を算出すると共に、算出した最大アクセス許容数をアクセス情報DB209に登録する。

#### 【0028】

ユーザクラス別アクセス要求読出手段205は、フィルタリング最適化手段204が、アクセスリスト109から最大アクセス許容数分のアクセス要求情報を読み出す際に、アクセスリスト109がユーザクラス別に登録されている場合、制御情報DB211から読み出す指針となる制御情報を抽出し、この制御情報に基づき、各ユーザクラスからアクセス要求情報を読み出す。有効タイマ設定手段203は、パケットフィルタリング設定情報を生成する際に、アクセス要求情報に有効タイマを設定する。

#### 【0029】

フィルタリング解除手段202は、有効タイマ満了時にネットワーク装置に設定したパケットフィルタリング制御を解除する。セッション完了フィルタリング解除手段208は、サービスサーバ300がユーザにサービスを提供する際に、セッション途中でユーザからのアクセスが不許可になることを防止するため、サービスサーバからセッションを終了したことを受信した際に、ネットワーク装置に設定したパケットフィルタリング制御を解除する。アクセス不許可フィルタリング設定手段201は、サービスサーバ300にアクセス不許可とするパケットフィルタリング設定情報を生成し、その情報をネットワーク装置20, 30に設定する。

#### 【0030】

サービスサーバ300において、セッション終了判定手段302は、ユーザとのセッションを終了したことを判定する。セッション終了通知手段301は、サービスサーバがユーザにサービスを提供する際に、セッション途中でユーザからのアクセスが不許可になるとを防止するため、ユーザとのセッションを終了したことをアクセス制御サーバ200に通知する。



## 【0031】

ここで、本発明方法のパケットフィルタリング機能について、図1の一部を抜粋した図2を用いて説明する。なお、図2～図9において、矢印に付した括弧付きの符号は文中の括弧付きの符号を対応させている。

## 【0032】

図2において、ユーザは、ユーザ端末50よりサービスサーバ300へのアクセス要求を受付サーバ100に送信する(1)。受付サーバ100のアクセス受付手段110は、アクセス要求情報を受信しアクセス登録手段103にその情報を渡す(2)。アクセス登録手段103は、受付順にアクセス要求情報をアクセスリスト109に登録する(3)。そして、アクセス制御サーバ200のフィルタリング最適化手段204にフィルタリング要求を行う(4)。

## 【0033】

そして、アクセス制御サーバ200のフィルタリング最適化手段204は、受付サーバ100のアクセス登録手段103からフィルタリング要求を受け、アクセス先のサービスサーバ300の処理能力に基づき静的アクセス許容数算出手段206で算出された(0)最大アクセス許容数をアクセス情報DB211より抽出し(5)、アクセスリスト109から最大アクセス許容数分のアクセス情報を読み出す(6)。次に、アクセス要求を行ったユーザ端末50のサービスサーバ300に対するアクセスを許可するパケットフィルタリング許可情報を生成し、パケットフィルタリング許可要求をトラヒック制御手段に行う(7)。トラヒック制御手段210は、それら情報に基づいてネットワーク装置20, 30を制御する(8)。

## 【0034】

また、上記の説明では、アクセス登録手段103は受付順にアクセス要求情報をアクセスリスト109に登録したが、別手段として、アクセス登録手段103は、ユーザクラス別アクセス登録を行う必要があれば、ユーザクラス別アクセス登録手段108にユーザクラス別アクセス登録要求を行う(3-1)。ユーザクラス別アクセス登録手段108は、ユーザクラスの間合わせをユーザクラス抽出手段102に行う(3-2)。

## 【0035】

ユーザクラス抽出手段102は、前記アクセス要求情報からIPアドレスを抽出し、IPアドレスによりユーザを特定し、ユーザプロファイル111からユーザクラスを抽出し（3-3）、抽出したユーザクラスをユーザクラス別アクセス登録手段108に返す（3-4）。そして、ユーザクラス別アクセス登録手段108は、取得したユーザクラスに基づいて、アクセス要求情報をアクセスリスト109に登録する（3-5）。

## 【0036】

次に、本発明方法の予測待合時間通知機能について、図1の一部を抜粋した図3を用いて説明する。

## 【0037】

図3において、ユーザは、ユーザ端末50よりサービスサーバ300へのアクセス要求を受付サーバに送信する（1）。アクセス受付手段110は、受信したアクセス要求をアクセスリストに登録するようアクセス登録手段103に要求する（2）。アクセス登録手段103は、空きのアクセスリスト109がない過負荷の場合、予測待合時間算出手段108へ予約待合時間算出要求をする（3）。予測待合時間算出手段108は、アクセスリスト109を参照し、本アクセス要求情報の登録位置に応じた待ち合わせを行っているユーザ数から予測待合時間を算出し、アクセス情報通知手段へユーザ通知要求をする（4）。アクセス情報通知手段107は、アクセス要求対象ユーザのユーザ端末50に対して、予測待合時間を通知する（5）。

## 【0038】

次に、本発明方法の予測待合時間通知機能について、図1の一部を抜粋した図4を用いて説明する。

## 【0039】

図4において、ユーザはユーザ端末50よりサービスサーバ300へのアクセス要求を受付サーバ100に送信する（1）。アクセス受付手段110は、受信したアクセス要求をアクセスリスト109に登録するようアクセス登録手段103に要求する（2）。アクセス登録手段103は、アクセス要求情報をアクセス

リスト 1 0 9 に登録するか否かを確認する場合、つまり、待ち合わせが必要である場合は、アクセス確認手段 1 0 4 にアクセスリスト 1 0 9 の登録確認を行う（3）。アクセス確認手段 1 0 4 は、アクセス要求情報からユーザ端末 5 0 の IP アドレスを抽出し、抽出した IP アドレスにアクセスリスト登録確認通知を行うよう待合せ確認通知手段 1 0 5 に要求する（4）。待合せ確認通知手段 1 0 5 はユーザに確認メッセージを送信する（5）。

## 【0 0 4 0】

そして、ユーザは確認メッセージの応答をアクセス受付手段 1 1 0 に再度送信する（6）。アクセス受付手段 1 1 0 は、ユーザからの応答をアクセス登録手段 1 0 3 に送信し（7）、アクセス登録手段 1 0 3 は、ユーザからの応答が登録ならば、アクセスリスト 1 0 9 にアクセス要求情報を登録する（8）。

## 【0 0 4 1】

次に、本発明方法の動的アクセス許容数算出機能について、図 1 の一部を抜粋した図 5 を用いて説明する。

## 【0 0 4 2】

図 5 において、動的アクセス許容数算出手段 2 0 7 は、周期的に負荷・トラフィック監視装置 2 1 2 からサービスサーバ 3 0 0 の負荷状態、及びサービスサーバ 3 0 0 を収容するネットワーク装置のトラフィック状態の情報を抽出し、最大アクセス許容数を算出する（1）。そして、その最大アクセス許容数をアクセス情報 DB に設定する（2）。

## 【0 0 4 3】

次に、本発明方法のユーザクラス別アクセス要求読出機能について、図 1 の一部を抜粋した図 6 を用いて説明する。

## 【0 0 4 4】

図 6 において、ユーザクラス別にアクセスリスト 1 0 9 にアクセス要求情報を登録する場合は、アクセス登録手段 1 0 3 は、ユーザクラス別にアクセス要求情報を登録する要求をユーザクラス別アクセス登録手段 1 0 8 に行う（1）。ユーザクラス別アクセス登録手段 1 0 8 は、ユーザクラス別にアクセスリスト 1 0 9 にアクセス要求情報の登録をする（2）。そして、アクセス登録手段 1 0 3 は、

フィルタリング最適化手段 2 0 4 にフィルタリング要求を行う (3)。

【 0 0 4 5 】

フィルタリング要求を受けたフィルタリング最適化手段 2 0 4 は、ユーザクラス別にどのような割合でアクセス要求情報を読み出すかを、ユーザクラス別アクセス要求読出手段 2 0 5 に問い合わせる (4)。ユーザクラス別アクセス要求読出手段はアクセス情報 DB から最大アクセス許容数を抽出し (5)、制御情報 DB からユーザクラス別にどのような割合でアクセス要求情報を読み出すかという制御情報を抽出し (6)、それらの情報に基づいて、ユーザクラス別にアクセス要求情報をアクセスリスト 1 0 9 から抽出し (7-1)、フィルタリング最適化手段に送信する (7-2)。

【 0 0 4 6 】

次に、本発明方法の有効タイマ機能について、図 1 の一部を抜粋した図 7 を用いて説明する。

【 0 0 4 7 】

図 7 において、受付サーバ 1 0 0 のアクセス登録手段 1 0 3 からフィルタリング要求をフィルタリング最適化手段 2 0 4 が受信すると (1-1)、フィルタリング最適化手段 2 0 4 は、ネットワーク装置 2 0, 3 0 にパケットフィルタリング設定後、有効タイマ設定手段 2 0 3 に有効タイマ設定要求を行う (1-2)。有効タイマ設定手段 2 0 3 は、アクセスリスト 1 0 9 のアクセス要求情報に有効タイマ値を設定する (1-3)。

【 0 0 4 8 】

フィルタリング解除手段 2 0 2 は、周期的にアクセスリスト 1 0 9 の有効タイマの満了チェックを行う (2-1)。有効タイマ満了アクセス要求情報があれば、アクセスリスト 1 0 9 からそのアクセス要求情報を削除し、該当アクセス要求を行ったユーザ端末をサービスサーバ 3 0 0 に対しアクセス許可からアクセス不許可とするパケットフィルタリング解除情報を生成し、トラヒック制御手段 2 1 0 に対してフィルタリング解除要求をする (2-2)。

【 0 0 4 9 】

次に、本発明方法のセッション終了機能について、図 1 の一部を抜粋した図 8

を用いて説明する。

【0050】

図8において、サービスサーバ300は、ユーザとのセッションが終了した際に、セッション終了判定手段302からのセッション終了通知をセッション終了通知手段301に通知する(1)。セッション終了通知手段301は、その旨をアクセス制御サーバ200のセッション完了フィルタリング解除手段208に送信する(2)。セッション完了フィルタリング解除手段208は、解除要求のあったコネクションに対して、ユーザ端末50からサービスサーバ300へのアクセスを許可から不許可とするパケットフィルタリング解除情報を生成し、トラヒック制御手段210に対してフィルタリング解除要求をする(3)。そして、トラヒック制御手段210は、パケットフィルタリング解除情報に基づいてネットワーク装置20, 30を制御する(4)。

【0051】

次に、本発明方法のアクセス不許可機能について、図1の一部を抜粋した図9を用いて説明する。

【0052】

図9において、ユーザは、ユーザ端末50よりサービスサーバ300へのアクセス要求を受付サーバ100のアクセス受付手段110に送信する(1)。アクセス受付手段110は、アクセス要求情報をユーザ認証手段101に送信する(2)。ユーザ認証手段101は、ユーザクラス抽出手段102を介して、ユーザプロフィール111よりアクセス要求を行ったユーザのユーザクラス(ユーザ情報)を抽出する(3)。その際に、対象ユーザがない場合や、ユーザクラスがアクセス不許可の場合は、アクセス不許可フィルタリング設定手段201に不許可のフィルタリング要求を行う(4-1)。

【0053】

アクセス不許可フィルタリング設定手段は、アクセス不許可のフィルタリング要求を受け、アクセス要求を行ったユーザ端末をサービスサーバ300にアクセス不許可とするパケットフィルタリング不許可情報を生成し、トラヒック制御手段210に対してフィルタリング不許可要求をする(4-2)。そして、トラヒ

ック制御手段 210 は、パケットフィルタリング不許可情報に基づいてネットワーク装置 20, 30 を制御する (5)。

【0054】

以下、本発明を用いた具体的なサービスの実施例を示し、処理の詳細を説明する。

【0055】

A. インターネットサービスプロバイダによる受付代行サービス

図 10 は、インターネットサービスプロバイダが受付代行サービスを行う実施例のシステム構成図を示す。図 10 に示すサイト (310) は、例えば人気商品のオンライン販売を予定しているサイトであり、アクセストラフィックの過度の集中が予想されている。このサイトはトラフィックの集中に備えて、サービスサーバ 300 を構成する数台のサーバ群 310 及び負荷分散装置 320 を準備しているが、販売開始直後のトラフィック集中に対してサーバの輻輳を懸念している。

【0056】

このサイトが加入しているサービスプロバイダはこのような、トラフィック集中が予想されるサイトに対して受付代行サービスを提供している。このサービスプロバイダは、受付サーバ 100 を構成する十分な台数の負荷分散サーバ群 120 及び負荷分散装置 130 と、アクセス制御サーバ 200 と、大容量の回線 220 からなる受付代行センタを構築している。

【0057】

ユーザ A, B のユーザ端末 51, 52 は、ネットワーク装置 20 としてのダイヤルアップルータ 21, 22 を介してコアネットワーク 10 に接続され、受付代行センタの負荷分散装置 130 はネットワーク装置 40 としてのルータ 41 に接続され、サイトの負荷分散装置 320 はネットワーク装置 30 としてのルータ 31 に接続されている。

【0058】

まず、この実施例で記述されるデータ・テーブル、及びメッセージ・テーブルについての説明をする。

## 【 0 0 5 9 】

図 1 1 は、ユーザプロファイル 1 1 1 のデータ構造を示す。ユーザプロファイル 1 1 1 は、ユーザ端末 5 1 の IP アドレスである送信元 IP アドレス ( 1 0 0 . 1 0 0 . 2 0 0 . 1 0 ) 、サービスサーバ 3 0 0 の IP アドレスである送信先 IP アドレス ( 1 0 0 . 1 0 0 . 4 0 0 . 1 0 0 ) 、サービスサーバ 3 0 0 のサービス提供通信ポート番号である送信先ポート番号 ( WWW を使ったサービスの場合は 8 0 であり、 h t t p を示す ) 、ユーザのサービス使用レベルの指標となるユーザクラス、例えば、高優先、中優先、低優先、不許可等のユーザクラスをデータとして設定される。このユーザプロファイルは送信元 IP アドレス及び送信先 IP アドレス毎に設定される。

## 【 0 0 6 0 】

図 1 2 は、アクセス情報 DB 2 0 9 のデータ構造を示す。アクセス情報 DB 2 0 9 は、例えばサービスサーバ 3 0 0 の IP アドレス ( 1 0 0 . 1 0 0 . 4 0 0 . 1 0 0 ) 、このサイトのサービスサーバ 3 0 0 が接続しているルータ ( ネットワーク装置 ) 5 1 の IP アドレス ( 1 0 0 . 1 0 0 . 4 0 0 . 1 ) 、パケットフィルタリングを設定する際のインタフェースを示すパケットフィルタリング機能種別 ( 例えば S N M P ) 、サイトのサーバの処理能力を示す処理能力データ、ポート単位の情報を示すポート情報からなる。

## 【 0 0 6 1 】

処理能力データはサービスサーバ 3 0 0 の処理能力を示すデータ・テーブル ( 例えば CPU 種別、搭載メモリサイズ等 ) であり、各データはパーセント表示される。例えば高速 CPU の場合は 1 5 0 として初期アクセス許容数を 1 . 5 倍して最大アクセス許容数に設定することを示し、低速 CPU の場合は 5 0 として初期アクセス許容数を 1 / 2 倍して最大アクセス許容数に設定することを示す。

## 【 0 0 6 2 】

ポート情報は、更にポート番号、初期アクセス許容数、最大アクセス許容数、有効タイマ値からなる。例えば、契約時にサイトに提示された情報が、最大アクセス数 = 1 0 0 、平均アクセス時間 = 5 分であった場合、ポート番号に 8 0 ( h t t p を示す ) 、最大アクセス許容数に 1 0 0 、有効タイマ値に 7 分 ( 5 分を補

正した値)を設定する。有効タイム値は、サービスサーバ300の管理者がサービスをユーザに提供する上で必要と思われるサーバとユーザとのコネクション時間である。有効タイム値は事前に受付代行センタにサービスサーバ300の管理者が申請するものである。

#### 【0063】

また、アクセス情報DB209はネットワーク装置をアクセス制御するために、ユーザ用のデータとしても使用されるが、その場合は、IPアドレス、ネットワーク装置IPアドレス、パケットフィルタリング機能種別のみのデータが設定されており、その他のデータは設定されていない。

#### 【0064】

図13は、アクセスリスト109のデータ構造を示す。アクセスリスト109は、サービスサーバ300のIPアドレスである送信先IPアドレス(100.100.400.100)、対象アプリケーションのポート番号である送信先ポート番号(例えば80)、優先制御の有無を示す優先制御フラグ、ユーザからサービスサーバ300へのアクセス要求をキューイングするアクセスリストから構成される。アクセスリストは、優先制御フラグが優先制御なしの場合に使用されるアクセスリストと、優先制御ありの場合に使用される優先度(高優先・中優先・低優先等)で分けられた高優先アクセスリスト、中優先アクセスリスト、低優先アクセスリストがある。

#### 【0065】

各アクセスリストは現在ユーザが対象とするサーバに接続可能かどうかを示す過負荷フラグ、接続中ユーザのキュー(バッファ・エリア)である接続中アクセスリストのポインタ、及び接続中アクセスリストにキューイングされている接続中のユーザ数である接続中ユーザ数、接続待ちユーザのキューである接続待ちリストのポインタ、及び接続待ちアクセスリストにキューイングされている接続待ちのユーザ数である接続待ちユーザ数からなる。

#### 【0066】

優先制御フラグは、サービスサーバ300の管理者がユーザクラス別の優先制御を希望する場合に、事前にサービスサーバ300の管理者が受付代行センタに



申請することで、優先制御フラグが優先制御ありで設定される。過負荷フラグは、現在ユーザがアクセスを要求するサーバに接続の空きがあるか否かを判定するためのフラグである。

## 【 0 0 6 7 】

また、空きバッファリストの先頭を示す空きバッファポインタ、有効タイマ切れの時刻でキューイングされている有効タイマ順ポインタがある。

## 【 0 0 6 8 】

図 1 4 は、制御情報 DB 2 1 1 を示す。制御情報 DB 2 1 1 は、受付代理センタが提供する優先制御を行う場合のユーザクラス数であるユーザクラス数（例えば、高優先・中優先・低優先の場合は、3 が設定される）、優先制御を希望するサービスサーバ 3 0 0 毎に設定される読出制御データが設定されている。読出制御データはサービスサーバ 3 0 0 の IP アドレスと、対象アプリケーションのポート番号であるポート番号毎にアクセスリスト 1 0 9 からユーザクラス別に読み出す比率である読出比率が設定されている。

## 【 0 0 6 9 】

次に、図 1 0 に示すインターネットサービスプロバイダが受付代行サービスを実施する場合について説明する。

## ( 1 ) 受付代行サービスの契約

図 1 0 に示すサイト service. com は、サービスプロバイダと受付代行サービスを契約する。契約時に service. com は、自サイトへの http アドレス、IP アドレス、自サイトのサーバ処理能力（最大処理数、一人あたりの平均アクセス時間等）をサービスプロバイダに提示する。

## 【 0 0 7 0 】

サービスプロバイダは、サイトから提示された情報を図 1 2 に示すアクセス情報 DB 2 0 9 に登録し、例えば、http://service.request.com といった URL をサイトへ発行する。URL の発行を受けたサイトはこの URL を、この URL の有効期間（受付代行サービスの契約期間）と共に、一般ユーザに公開する。

## 【 0 0 7 1 】

サービスプロバイダは、顧客であるサイトから具体的なアクセス数やアクセス時間を提示してもらう代わりに、制御情報DB 2 1 1の処理能力データから最大アクセス許容数を計算して設定するようにシステムを構築することも可能である。この場合の、静的アクセス許容数算出手段2 0 6が実行する処理のフローチャートを図1 5に示す。

#### 【0 0 7 2】

図1 5において、静的アクセス許容数算出手段2 0 6は、ステップS 2 0 6 1でアクセス情報DB 2 0 9から処理能力データを抽出する。次に、ステップS 2 0 6 2で抽出した処理能力データから最大アクセス許容数を計算する。この計算式としては、例えば、アクセス情報DB 2 0 9の処理能力データとして、高速CPUが搭載されている場合は、受付代行センタで定義されたCPU対応表等で、1 5 0 %というデータが設定され、大量にメモリを搭載している場合も、同じく受付代行センタの定義された搭載メモリ対応表等で、2 0 0 %というデータが設定されると、その平均を取って予め受付代行センタが定義している初期アクセス許容数から以下の計算等で、最大アクセス許容数を算出する。

$$(\text{初期アクセス許容数}) \times (1.5 + 2.0) / 2$$

最後にステップS 2 0 6 3で算出した最大アクセス許容数をアクセス情報DB 2 0 9に設定する。

#### (2) 受付代行サービス開始

サービスプロバイダは、保守コンソールなどを通じて受付代行サービス開始時刻直前に、プロバイダ管理下であるネットワークのエッジルータ、つまり、一般ユーザ用のダイヤルアップルータ2 1, 2 2や、他プロバイダと接続する境界ルータにサイトのIPアドレス1 0 0. 1 0 0. 4 0 0. 1 0 0へのアクセス規制を設定する。アクセス規制はルータ2 1, 2 2等において、指定されたIPアドレスを宛先とするIPパケットを棄却する事で行われる。この機能は一般にフィルタリングと呼ばれており、最近の多くのネットワーク装置がこの機能を備えている。設定インタフェースはネットワーク装置により異なるが、SNMPや独自のCLI（コマンドラインインタフェース）が用いられる。

#### 【0 0 7 3】

これにより受付代行サービス開始時刻を持って、ユーザは直接 `http://service.com` へアクセスできなくなり、このサイトへのアクセスは `http://service.request.com` を介したものが有効になる。

### (3) 受付代行センタでの処理概要

ユーザは、ユーザ端末 51, 52 よりインターネットブラウザから `http://service.request.com` を入力し、受付代行センタへアクセスする。受付代行センタは本発明によらない既存のサーバ負荷分散の仕組みを用いて、負荷分散サーバ群 120 いずれかのサーバにこの要求を回送する。

#### 【0074】

受付サーバ 100 は、既存のアクセス受付手段 110 を介して、`http` プロトコルを受信し、アクセス登録手段 103 にその情報を渡す。アクセス受付手段 110 は、具体的には受付専用のサーバアプリケーションであり、`html`, `Java`, その他のスクリプト言語等で記述される。このアプリケーション自体に、本発明の固有要素は無く、図 16 に示すようなアクセス要求情報を抽出し、例えばプロセス間通信を用いてアクセス登録手段 103 に情報を渡す。初回アクセス時、即ち `http://service.request.com` へのアクセス時は、要求種別にアクセス要求を設定する。

#### 【0075】

図 16 は、アクセス要求情報のメッセージ構造を示す。アクセス要求情報は、アクセス登録手段 103 に処理指標を示す要求種別（アクセス要求、待合せ応答要求、待合せ拒否要求）、ユーザ端末の IP アドレスである送信元 IP アドレス、サービスサーバ 300 の IP アドレスである送信先 IP アドレス、サービスサーバ 300 がユーザと通信を行うための対象アプリケーションのポート番号である送信先ポート番号からなる。

#### 【0076】

図 17、図 18 はアクセス登録手段 103 の処理を詳細に説明するためのフローチャートを示す。まず、アクセス登録手段 103 は、図 17 のステップ S1031 で受信したアクセス要求情報の要求種別を判断する。ここでは、アクセス要

求情報の要求種別はアクセス要求であるから、ステップS1032に分岐する。アクセス要求情報のIPアドレスとポート番号でアクセスリスト109を索引し、当該アクセスリストの接続状態を示す過負荷フラグを判定する。ここでは過負荷でないものとし、図18のステップS1038に分岐する。

## 【0077】

ただし、過負荷の場合は、ユーザに待合せを行うことの確認と、予測待合せ時間の通知を行うため、図17のステップS1034に分岐する。ユーザに待合せを行うことの確認と、予測待合せ時間の通知については、「受付代行センタでのユーザ通知」で後述する。

## 【0078】

ステップS1038では、抽出したアクセスリスト109の優先制御フラグを抽出し、ステップS1039で優先制御無しか否かを判定する。ここでは優先制御無しが設定されたものとし、ステップS10310に分岐する。優先制御ありの場合は、「サービスクラスによる優先制御サービス」で後述する。

## 【0079】

ステップS10310では図13に示すアクセスリスト109のバッファエリアの空きバッファを検索し、該当バッファに入力されたアクセス要求情報の接続元IPアドレス(100.100.200.10)を設定し、空きバッファポイントの更新を行う。ステップS10311で新たに捕捉したバッファを接続待ちアクセスリスト109にキューイングし、ステップS10312でアクセスリスト109の接続待ちユーザ数を更新する。キューイングの制御については、本発明とは直接関係しないので、説明を省略する。

## 【0080】

次に、ステップS10313で、図19に示すフィルタリング要求のフィルタリング要求種別に許可要求を設定し、その他の情報をアクセス要求情報から複写して設定し、フィルタリング最適化手段204に制御を渡す。

## 【0081】

図19は、フィルタリング要求のメッセージ構造を示す。フィルタリング要求は、フィルタリング最適化手段204に処理指標を示す要求種別(許可要求、不

許可要求、優先制御付き許可要求、アクセス許可を解除するための解除要求)、ユーザ端末のIPアドレスである送信元IPアドレス、サービスサーバ300のIPアドレスである送信先IPアドレス、サービスサーバ300がユーザと通信を行うための対象アプリケーションのポート番号である送信先ポート番号からなる。

#### 【0082】

図20、図21はフィルタリング最適化手段204の処理を詳細に説明するためのフローチャートを示す。この処理は、実際にはアクセス情報DB209に登録された全インスタンスについて実行されるが、ここでは説明を簡単にするために1インスタンスの処理のみを記述する。

#### 【0083】

まず、フィルタリング最適化手段204は、図20のステップS2041で入力されたフィルタリング要求のフィルタリング要求種別を判定する。フィルタリング要求種別が許可要求であれば、ステップS2042に分岐する。優先制御付き許可要求であれば、ユーザクラス別にアクセス要求を読み出す。ユーザクラス別にアクセス要求を読み出す手段については、「サービスクラスによる優先制御サービス」で後述する。

#### 【0084】

ステップS2042ではアクセス情報DB209よりポート番号対応に最大アクセス許容数を抽出する。次に、ステップS2043でアクセスリスト109より過負荷フラグを抽出し、ステップS2044で過負荷フラグを判定し、接続空き無しであれば処理を終了する。

#### 【0085】

過負荷フラグが接続空き有りの場合は、ステップS2045でアクセスリスト109の接続中ユーザ数を抽出し、ステップS2046で最大アクセス許容数から接続中ユーザ数を差し引いた分、接続待ちアクセスリスト109から送信元IPアドレスを抽出し、内部データの新規アクセス許可リストに設定する。新規アクセス許可リストは、接続待ちアクセスリスト109から抽出した送信元IPアドレスで構成される。この後、ステップS2047で有効タイマ設定手段203

を起動してステップ S 2 0 4 1 2 に進む。有効タイマ設定手段 2 0 3 については後述する。

#### 【 0 0 8 6 】

図 2 1 のステップ S 2 0 4 1 2 では、内部データの新規アクセス許可リストが無くなるまでループ処理を行う。ステップ S 2 0 4 8 では、アクセス情報 DB 2 0 9 よりアクセス許可対象 IP アドレスに対するネットワーク装置の IP アドレスとパケットフィルタリング機能種別を抽出する。そして、ステップ S 2 0 4 9 でパケットフィルタリング機能種別に対応した許可フィルタリング・コマンドを作成する。ステップ S 2 0 4 1 0 で、作成した許可フィルタリング・コマンドと、ステップ S 2 0 4 8 で抽出したネットワーク装置の IP アドレスとを図 2 2 に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段 2 1 0 に制御を渡す。そして、ステップ S 2 0 4 1 3 で処理済みアクセス許可対象 IP アドレスを削除する。

#### 【 0 0 8 7 】

図 2 2 は、フィルタリング・コマンド実行要求のメッセージ構造を示す。フィルタリング・コマンド実行要求は、フィルタリングを実行するネットワーク装置の IP アドレスとフィルタリング・コマンドフィールドからなる。フィルタリング・コマンドフィールドは、例えばユーザ端末 5 1 ( 1 0 0 . 1 0 0 . 2 0 0 . 1 0 ) からサービスサーバ 3 0 0 ( 1 0 0 . 1 0 0 . 4 0 0 . 1 0 0 ) に WWW ( http ) でのアクセスを不許可にする場合は、`「ipchains -s 100.100.200.10 -d 100.100.400.100 -p http -j DENY」`という実行可能レベルのコマンドが設定されている。

#### 【 0 0 8 8 】

図 2 3 は、トラヒック制御手段 2 1 0 の処理を詳細に説明するためのフローチャートを示す。まず、トラヒック制御手段 2 1 0 は、ステップ S 2 1 0 1 で入力されたフィルタリング・コマンド実行要求の IP アドレスに対して、Telnet 等を用いて通信ポートを開く。次に、ステップ S 2 1 0 2 で開いた通信ポートを介し、入力されたフィルタリング・コマンド実行要求のフィルタリング・コマ

ンドを起動する。ここでは、許可フィルタリング・コマンドを起動することで、ユーザは直接 `http://service.com` に対しアクセス可能となる。

#### (4) 受付代行センタでのアクセス許可解除

ここでは、直接 `http://service.com` にアクセス可能となったユーザのアクセス許可を解除する実施例を示す。

##### 【0089】

受付代行センタは、アクセス許可を解除する手段として、サービスサーバ300へのアクセス有効タイマが満了した時に解除する手段と、サービスサーバ300とユーザとのサービス・セッション、例えば、ユーザが購入した動画データをダウンロードするセッション、インターネット・ショッピングにおける購入手続きのセッション、が終了した時にサービスサーバ300から受付代行センタへサービス・セッションが終了したことを通知することによる解除手段とを備えている。

##### 【0090】

サービスサーバ300へのアクセス有効タイマ満了による解除手段は、フィルタリング最適化手段204の処理の中で起動する有効タイマ設定手段203であり、有効タイマ値をアクセスリスト109に設定する。

##### 【0091】

図24は、有効タイマ設定手段203の処理を詳細に説明するためのフローチャートを示す。まず、有効タイマ設定手段203は、ステップS2031でアクセス情報DB209より入力された有効タイマ設定要求の送信先IPアドレスと送信先ポート番号に対する有効タイマ値を抽出する。次に、ステップS2032で入力された有効タイマ設定要求の要求種別が優先制御有るか、無しかを判定する。ここでは優先制御無しが設定されているものとし、ステップS2033に分岐する。

##### 【0092】

ステップS2033では、入力された有効タイマ設定要求の最大アクセス許容数と接続中ユーザ数の差分分を符合せアクセスリスト109から接続中アクセス

リスト 1 0 9 にキューを移す。ステップ S 2 0 3 4 で先のステップ S 2 0 3 1 で抽出した有効タイマ値を、現時刻に加算する。ステップ S 2 0 3 5 では接続中アクセスリスト 1 0 9 に移されたキューが持つ有効タイマ値に、先のステップ S 2 0 3 4 で算出された値を設定する。

#### 【 0 0 9 3 】

例えば、アクセス情報 DB 2 0 9 から抽出した有効タイマ値が 7 分で、現時刻が 7 時 3 0 分ならば、7 時 3 7 分となり、サービスサーバ 3 0 0 へのアクセス許可が解除される時刻が 7 時 3 7 分ということを示す。次に、ステップ S 2 0 3 6 で上記解除される時刻が設定されたバッファ・エリアをアクセスリスト 1 0 9 の有効タイマ順ポインタにキューイングする。そして、ステップ S 2 0 3 7 でアクセス情報 DB 2 0 9 の入力された有効タイマ設定要求の送信先 IP アドレスと送信先ポート番号に対する接続中ユーザ数を加算して、接続待ちユーザ数を減算する。

#### 【 0 0 9 4 】

有効タイマ手段 2 0 3 によってユーザがサービスサーバ 3 0 0 へアクセスするアクセス可能な時間が設定されるので、フィルタリング解除手段 2 0 2 はアクセス可能な時間が満了していないかを周期的に確認を行い、アクセス可能な時間が満了していた場合は、ユーザのサービスサーバ 3 0 0 へのアクセス許可を解除する。

#### 【 0 0 9 5 】

図 2 5 は、フィルタリング解除手段 2 0 2 の処理を詳細に説明するためのフローチャートを示す。フィルタリング解除手段 2 0 2 は、ある一定の周期でシステムを構築した OS（オペレーション・システム）が持つタイマ起動で呼び出される。まず、ステップ S 2 0 2 1 でアクセスリスト 1 0 9 の有効タイマ順ポインタによりキューイングされたキューから有効タイマ切れの送信元 IP アドレスを抽出し、ステップ S 2 0 2 2 でアクセスリスト 1 0 9 の有効タイマ順ポインタによりキューイングされたキューから上記抽出した分を削除する。

#### 【 0 0 9 6 】

次に、ステップ S 2 0 2 3 でアクセス情報 DB 2 0 9 より先のステップ S 2 0



21で抽出したアクセス解除対象のIPアドレスに対するネットワーク装置のIPアドレスとパケットフィルタリング機能種別を抽出する。そして、ステップS2024でアクセスリスト109の有効タイマ順ポインタによりキューイングされたキューから先のステップS2021で抽出した分を、接続中アクセスリスト109から空きバッファ・キューに移し、接続中ユーザ数を減算する。

#### 【0097】

次に、ステップS2025でパケットフィルタリング機能種別に対応したアクセス許可を解除するフィルタリング・コマンドを作成し、ステップS2026で作成した解除フィルタリング・コマンドと、先のステップS2023で抽出したネットワーク装置のIPアドレスとを図22に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段210に制御を渡す。トラヒック制御手段210によってアクセス許可を解除するフィルタリング・コマンドを起動することで、ユーザは直接http://service.comへアクセスが出来なくなる。

#### 【0098】

次に、受付代行センタが備えるもう一つの解除手段、サービスサーバ300とユーザとのサービス・セッションが終了した時にサービスサーバ300から受付代行センタへサービス・セッションが終了したことを通知することによる解除手段を説明する。

#### 【0099】

サービスサーバ300は、例えば、ユーザが購入した動画データをダウンロードするセッション、インターネット・ショッピングにおける購入手続きのセッションのような通信を途中で切断されて困る場合は、サービスプロバイダと受付代行サービスを契約する際に、提示する自サイトのサーバ処理能力を示す一人当たりの平均アクセス時間を長く設定しておき、周期的にアクセス解除する手段に頼らず、サービスサーバ300が図26のセッション終了通知手段301によりアクセス解除する手段を利用できる。

#### 【0100】

図26は、セッション終了通知手段301の処理を詳細に説明するためのフロ

ーチャートを示す。サービスサーバ300は、既存のセッション終了判定手段302を用いてセッション終了を判定し、図27に示すセッション終了通知メッセージのサービスサーバ300 IPアドレスに自IPアドレス、サービスサーバ300ポート番号に、ユーザとのセッションに使用したポート番号、クライアントIPアドレスにセッションを行ったユーザのIPアドレスを設定し、セッション終了通知手段301を起動する。これにより、セッション終了通知手段301は、図26のステップS3011でアクセス制御サーバのセッション完了フィルタリング解除手段208に入力されたセッション終了通知を送信する。

#### 【0101】

図27は、セッション終了通知のメッセージ構造を示す。セッション終了通知は、サービスサーバ300のIPアドレスであるサービスサーバIPアドレス、ユーザとのセッションに使用したポート番号であるサービスサーバポート番号、セッションを行ったユーザのIPアドレスであるクライアントIPアドレスからなる。

#### 【0102】

図28は、セッション完了フィルタリング解除手段208の処理を詳細に説明するためのフローチャートを示す。セッション完了フィルタリング解除手段208は、サービスサーバ300からのセッション終了通知を受けるべく、ある通信ポートを開いてメッセージ受信待ちとなっている。まず、ステップS2081でアクセス情報DB209より入力されたセッション終了通知のクライアントIPアドレスに対するネットワーク装置のIPアドレスとパケットフィルタリング機能種別を抽出する。そして、ステップS2082でアクセスリスト109から入力されたセッション終了通知のサービスサーバ300のIPアドレス、サービスサーバ300ポート番号、クライアントIPアドレスに対するアクセス許可解除対象のバッファ・エリアを接続中アクセスリスト109のキューから空きバッファのキューに変更し、接続中ユーザ数を減算する。

#### 【0103】

次に、ステップS2083でパケットフィルタリング機能種別に対応したアクセス許可を解除するフィルタリング・コマンドを作成する。次に、ステップS2

084で作成した解除フィルタリング・コマンドと、先のステップS2081で抽出したネットワーク装置のIPアドレスとを図22に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段210に制御を渡す。これにより、トラヒック制御手段210によってアクセス許可を解除するフィルタリング・コマンドを起動することで、ユーザは直接http://service.comへアクセスが出来なくなる。

#### (5) 受付代行センタでのユーザ通知

受付代行センタはユーザに対して待合せを行うことの確認、及び予測待合せ時間の通知を、サービスサーバ300が過負荷か否かを判断し(図17のステップS1033)、過負荷の場合には、アクセスリスト109に登録する処理の前に行う。

#### 【0104】

最初に待合せを行うことをユーザに確認する手段について説明する。図29は、アクセス確認手段104の処理を詳細に説明するためのフローチャートを示す。図30は、待合せ確認通知手段105の処理を詳細に説明するためのフローチャートを示す。ユーザは、ユーザ端末よりサービスサーバ300へのアクセス要求を受付サーバ100のアクセス受付手段110に送信する。アクセス受付手段110は、受信したアクセス要求をアクセスリスト109に登録するようアクセス登録手段103に要求する。アクセス登録手段103は、アクセス要求情報をアクセスリスト109に登録するか否かを確認する場合(過負荷の場合:図17のステップS1033で判断する)、アクセス確認手段104にアクセスリスト登録確認を行う。

#### 【0105】

アクセス確認手段104は、図29のステップS1041において、アクセス確認を行うための確認メッセージを作成する。次に、ステップS1042で作成した確認メッセージを待合せ確認通知手段105に処理を渡す。待合せ確認通知手段105は、図30のステップS1051において、確認メッセージをHTTPプロトコルでユーザに通知する。そして、ユーザは確認メッセージの応答をアクセス受付手段110に再度送信する。アクセス受付手段110は、ユーザから

の応答をアクセス登録手段103に送信し、アクセス登録手段103はユーザからの応答が登録ならば（図17のステップS1031で判断する）、アクセスリスト109にアクセス要求情報を登録する。

#### 【0106】

次に予測待合せ時間を通知する手段を説明する。図31は、予測待合せ時間算出手段106の処理を詳細に説明するためのフローチャートを示す。図32は、アクセス情報通知手段107の処理を詳細に説明するためのフローチャートを示す。ユーザは、ユーザ端末よりサービスサーバ300へのアクセス要求を受付サーバ100のアクセス受付手段110に送信する。アクセス受付手段110は、受信したアクセス要求をアクセスリスト109に登録するようアクセス登録手段103に要求する。アクセス登録手段103は、空きのアクセスリスト109がない過負荷の場合（図17のS1033で判断する）、予測待合せ時間算出手段106へ予約待合せ時間算出要求をする。

#### 【0107】

予測待合せ時間算出手段106は、図31のステップS1061において、アクセスリスト109より入力されたアクセス要求情報の送信先IPアドレスと送信先ポート番号に対する待合せアクセスリスト109のユーザ数と有効タイマ値を抽出し、有効タイマ値とユーザ数の乗算を行い待合せ時間を算出し、ステップS1062で予測待合せ時間を通知するメッセージを作成する。そして、ステップS1063で作成した予測待合せ時間を通知するメッセージをアクセス情報通知手段107に処理を渡す。アクセス情報通知手段107は、図32のステップS1071で予測待合せ時間を通知するメッセージをHTTPプロトコルでユーザに通知する。

#### 【0108】

##### B. インターネットサービスプロバイダによる最適アクセスサービス

また、本発明は、前述の図15を用いて説明した静的アクセス許容数算出手段206だけでなく、図33の動的アクセス許容数算出手段207によって、サーバのCPU使用率、ネットワーク使用率を考慮してサービスサーバ300への最大アクセス許容数を動的に変更する。

## 【 0 1 0 9 】

図 3 3 は、動的アクセス許容数算出手段 2 0 7 の処理を詳細に説明するためのフローチャートを示す。以下、既存の負荷・トラヒック監視装置 2 1 2 用いて、周期的にサービスサーバ 3 0 0 の負荷状態、及びサービスサーバ 3 0 0 を収容するネットワーク装置のトラフィック状態の情報を抽出し、最大アクセス許容数を変更することで、実際の処理負荷やネットワークのトラヒックに対するアクセスを許容可能とする手段について説明する。

図 3 3 において、動的アクセス許容数算出手段 2 0 7 は、ステップ S 2 0 7 1 で周期的に負荷・トラヒック監視装置 2 1 2 からサービスサーバ 3 0 0 の負荷状態、及びサービスサーバ 3 0 0 を収容するネットワーク装置のトラフィック状態の情報を抽出し、各データの平均値を算出する。例えば、CPU 使用率 8 0 %、トラヒック量がサーバ・許容トラヒック量（ワイヤ・スピード）に対しての使用量 9 0 % の場合、平均値は 8 5 % となる。

## 【 0 1 1 0 】

ステップ S 2 0 7 2 ではアクセス情報 DB 2 0 9 から現在設定されている最大アクセス許容数を抽出し、現在の CPU 使用量、及びトラヒック量にあった最大アクセス許容数を算出する。本発明はその算出方法については特定しないが、例えば、ステップ S 2 0 7 1 で算出された平均値が 8 5 % であれば、その算出方法は、8 0 % 以上の場合だけ変更を行い、以下の計算を行う。

$(\text{抽出した最大アクセス許容数}) \times [1 - (0.85 - 0.8)]$

そして、ステップ S 2 0 7 3 で、その最大アクセス許容数をアクセス情報 DB 2 0 9 に設定する。

## 【 0 1 1 1 】

C. インターネットサービスプロバイダによるサービスクラスによる優先制御サービス

前記 A ( 1 ) の受付代行サービスの契約時に契約するサービスサーバ 3 0 0 がユーザクラスによる優先制御を行うかどうかをサービスサーバ 3 0 0 の契約者は選択できる。優先制御を行う場合は、アクセスリスト 1 0 9 内の優先制御の有無を示す優先制御フラグを優先制御ありを示すフラグを設定しておくことで、サー

ビスサーバ300へのアクセス許可が高優先のユーザから優先的に許可可能となる。

#### 【0112】

前記A(3)で説明したアクセス登録手段103は、サービスサーバ300が優先制御ありかどうかを判断し、優先制御ありならば、図34に示すユーザクラス別アクセス登録手段108で、ユーザクラス別にアクセスリスト109にアクセス要求情報を登録する。

#### 【0113】

図34は、ユーザクラス別アクセス登録手段108の処理を詳細に説明するためのフローチャートを示す。ユーザクラス別アクセス登録手段108は、ステップS1081でユーザプロファイル111から図35(A)に示す処理手順のユーザクラス抽出手段102を用いてユーザクラスを抽出する。ここでは、図35(B)に示すように、入力されたアクセス要求情報の送信元IPアドレスを用いてユーザプロファイル111を検索してユーザクラスを抽出する。

#### 【0114】

次に、ステップS1082でバッファエリアの空きバッファキューを検索し、該当バッファに接続元IPアドレスを設定し、バッファエリアの空きバッファキューを更新し、ステップS1083で新たに捕捉したバッファを接続待ちアクセスリスト109にキューイングする。そして、ステップS1084でアクセスリスト109の接続待ちユーザ数を加算する。キューイングの制御については、本発明とは直接関係しないので説明を省略する。その後、ステップS1085で、図19に示すフィルタリング要求のフィルタリング要求種別に優先制御付き許可要求を、その他の情報をアクセス要求情報から複写して設定、フィルタリング最適化手段204に制御を渡す。

#### 【0115】

これにより、フィルタリング最適化手段204は、アクセスリスト109から最大アクセス許容数分のアクセス情報を読み出す際に、入力されたフィルタリング要求のフィルタリング要求種別を判断し(図20のステップS2041)、優先制御付き許可要求の場合、ユーザクラス別アクセス要求読出手段205を起動

する（図20のステップS20411）。そして、出力されたIPアドレスを内部データ新規アクセス許可リストに設定する。

#### 【0116】

図36は、ユーザクラス別アクセス要求読出手段205の処理を詳細に説明するためのフローチャートを示す。ユーザクラス別アクセス要求読出手段205は、ステップS2051でアクセス情報DB209より送信先IPアドレスと送信先ポート番号対する最大アクセス許容数を抽出する。次に、ステップS2052でアクセスリスト109より過負荷フラグを抽出する。そして、ステップS2054で過負荷フラグを判定し、接続空き無しであれば処理を終了する。接続空き有りであればステップS2053に分岐する。

#### 【0117】

ステップS2053では、制御情報DB211から入力されたフィルタリング要求の送信先IPアドレスと送信先ポート番号に対する読出比率を抽出する。例えば、読出比率が3:2:1ならば、高優先リストから割合1/2で、中優先リストから1/3で、低優先リストから1/6の比率でアクセス要求情報をアクセスリスト109から読み出すことを示す。

#### 【0118】

次に、ステップS2055で入力されたフィルタリング要求の送信先IPアドレスと送信先ポート番号に対する各ユーザクラスの接続中ユーザ数を抽出する。ステップS2056で先にステップS2053で抽出した読出比率でアクセスリスト109からアクセス要求情報を読み出し、ステップS2057で有効タイマ設定手段203を起動する。そして、抽出したアクセス要求情報の送信元IPアドレスを呼び元に返す。このようにして、ユーザクラス別にアクセス要求情報をアクセスリスト109から抽出する。

#### 【0119】

図37は、有効タイマ設定要求のメッセージ構造を示す。有効タイマ設定要求は、優先制御ありか否かを示す要求種別、最大アクセス許容数と接続中ユーザとの差分、サービスサーバ300のIPアドレスである送信先IPアドレス、サービスサーバ300がユーザと通信を行うための対象アプリケーションのポート番

号である送信先ポート番号からなる。最大アクセス許容数と接続中ユーザとの差分は、優先制御なしの場合は、データは1つであるが、優先制御ありの場合、ユーザクラスの種類分データが設定されている。例えば、高優先、中優先、低優先の場合は、3つのデータが設定されている。

#### 【0120】

D. インターネットサービスプロバイダによる不許可ユーザ規制サービス

前述のA(1)の受付代行サービスの契約で説明したように、サービスプロバイダは、サービスを提供するサービスサーバ300に例えば、`http://service.request.com`といったURLをサイトへ発行する。そして、URLの発行を受けたサイトはこのURLを、このURLの有効期間(受付代行サービスの契約期間)と共に、一般ユーザへ公開する。

#### 【0121】

サービスを提供するサーバは、URL公開の前にユーザとのサービス契約を結び、そのユーザからのアクセスのみをユーザプロファイル111にアクセス許可として登録し、契約していないユーザに対しては不許可ユーザとして登録することが可能である。ユーザプロファイル111に登録された不許可ユーザからのアクセスは、サービスサーバ300の代わりに受付代理センタがユーザ認証を行い、不許可ユーザからサービスサーバ300へアクセスを未然に防止することで、サービスサーバ300に余分な負荷を及ぼさない。

#### 【0122】

ユーザ端末よりサービスサーバ300へのアクセス要求があると、アクセス受付手段110は、ユーザ認証手段101へアクセス要求情報を通知する。

#### 【0123】

図38は、ユーザ認証手段101の処理を詳細に説明するためのフローチャートを示す。また、図39はアクセス不許可フィルタリング設定手段201の処理を詳細に説明するためのフローチャートを示す。

#### 【0124】

ユーザ認証手段101は、図38のステップS1010で入力されたアクセス要求情報の要求種別を判定し、要求種別がアクセス要求であればステップS10



11に分岐し、アクセス要求で無ければステップS1015でアクセス要求情報をアクセス登録手段103に引き渡す。

#### 【0125】

ステップS1011では、アクセス要求情報の送信元IPアドレスのユーザクラスをユーザプロファイル111からユーザクラス抽出手段102を介してユーザクラスを抽出する。そして、ステップS1012で抽出したユーザクラスを判定し、アクセス不許可の場合は、ステップS1013に分岐してフィルタリング要求種別を不許可とするフィルタリング要求を、アクセス不許可フィルタリング設定手段201に引き渡す。一方、アクセス許可の場合は、ステップS1014でアクセス要求情報をアクセス登録手段103に引き渡す。

#### 【0126】

図20において、アクセス不許可フィルタリング設定手段201は、ステップS2011でアクセス情報DB209より入力されたフィルタリング要求の送信先IPアドレスに対するネットワーク装置のIPアドレスとパケットフィルタリング機能種別を抽出し、ステップS2012でパケットフィルタリング機能種別に対応した不許可フィルタリング・コマンドを作成する。ステップS2013では、作成した不許可フィルタリング・コマンドと、先のステップS2011で抽出したネットワーク装置のIPアドレスとを図22に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段210に制御を渡す。このトラヒック制御手段210によって不許可フィルタリング・コマンドを起動することで、ユーザは直接http://service.comへアクセスが出来なくなる。

#### 【0127】

本発明においては、常時、サーバの能力を効果的に引き出すためにサービスサーバ300が処理可能な分のユーザがサービスサーバ300に直接アクセスする方法をとっているため、プロキシ・サーバのキャッシュ機能を用いた際に発生するコンテンツが更新されない課題や、アクセスする度に内容が変化する動的オブジェクトが再利用できないという課題が解決されると共に、無意味なトラヒックがコアネットワーク10に流さないため、トラヒックの軽減も図ることができ

る。さらに、トラフィック量を軽減することにより、ネットワーク・リソースの有効活用も可能とする。

【0128】

本発明においては、ユーザからのアクセス要求の待合せを可能としており、サービスサーバ300で接続コネクション数を設定した場合に比べてユーザに与える負担も軽減される。さらに、本発明ではサービスサーバ300の負荷状況やトラフィック状況を定期的に監視しているので、接続先のサービスサーバ300の処理能力を把握でき、サービスサーバ300が最適に動作可能なアクセス分のユーザにアクセスを許可することが可能となる。

【0129】

さらに、現状では、ユーザが高トラフィック、または過負荷なサービスサーバにアクセスした場合、応答速度が遅かったり、散々応答を待った挙げ句アクセスを拒否する旨のメッセージが送信されるという問題があるが、本発明を適用すると待合せが可能であるため、アクセス要求したユーザは自分のアクセス順番になれば、速い応答速度で快適にサービスを受けることが可能となる。

【0130】

さらに、本発明が必要となるような接続要求輻輳時に本発明によるアクセス制御を行い、非輻輳状態においては、従来技術による通常接続制御を行う、というように常に最良の接続性を保証することも可能である。

【0131】

(付記1) パケットフィルタリング機能を有するネットワーク装置と、  
前記ネットワーク装置を介してIPネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介してIPネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記IPネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付ける受付サーバと、

前記ネットワーク装置を制御するアクセス制御サーバと、で構成されるネットワークシステムのネットワークアクセス制御方法において、

前記受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うことを特徴とするネットワークアクセス制御方法。

#### 【 0 1 3 2 】

(付記 2) パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介して IP ネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介して IP ネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記 IP ネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付けるアクセス受付手段を備えた受付サーバと、

前記ネットワーク装置を制御するトラヒック制御手段を備えたアクセス制御サーバと、で構成されるネットワークシステムにおいて、

前記受付サーバは、前記アクセス受付手段を介しユーザ端末からのアクセス要求情報を受信して保持するアクセス登録手段を有し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うフィルタリング最適化手段を有することを特徴とするネットワークシステム。

#### 【 0 1 3 3 】

(付記 3) ユーザ端末からのアクセス要求情報を保持するアクセスリストと、

各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロフィールと、

ユーザ端末からのアクセスを受け付けるアクセス受付手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリスト

に受付順に登録するアクセス登録手段と、

受信したアクセス要求情報から I P アドレスを抽出し、I P アドレスによりユーザを特定して前記ユーザプロファイルからユーザクラスを抽出するユーザクラス抽出手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザクラス別アクセス登録手段を

有することを特徴とする受付サーバ。

#### 【 0 1 3 4 】

(付記 4) 付記 3 記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位置に応じた待ち合わせを行っているユーザ数から予測待ち合わせ時間を算出する予測待ち時間算出手段と、

算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を有することを特徴とする受付サーバ。

#### 【 0 1 3 5 】

(付記 5) 付記 3 記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するアクセス確認手段と、

前記アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を有することを特徴とする受付サーバ。

#### 【 0 1 3 6 】

(付記 6) サービスサーバの処理能力に関する情報及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持するアクセス情報データベースと、

ネットワーク装置を制御するトラヒック制御手段と、

前記サービスサーバの処理能力に関する情報に基づき最大アクセス許容数を算

出する静的アクセス許容数算出手段と、

受付サーバでユーザ端末からのアクセス要求情報を保持するアクセスリストの先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバにアクセス可能とするパケットフィルタリング設定情報を生成し前記トラヒック制御手段を介して前記ネットワーク装置に設定するフィルタリング最適化手段を

有することを特徴とするアクセス制御サーバ。

#### 【0137】

（付記7） 付記6記載のアクセス制御サーバにおいて、

前記サービスサーバの負荷状態及びサービスサーバを収容するネットワーク装置のトラフィック状態を監視する負荷・トラヒック監視装置と、

周期的に負荷・トラヒック監視装置と通信して前記負荷状態及びトラヒック状態の情報を抽出して前記アクセス情報データベースの最大アクセス許容数を算出すると共に、算出した最大アクセス許容数を前記アクセス情報データベースに登録する動的アクセス許容数算出手段を

有することを特徴とするアクセス制御サーバ。

#### 【0138】

（付記8） 付記6記載のアクセス制御サーバにおいて、

ユーザ端末からのアクセス要求情報を前記アクセスリストから読み出す際に読み出す指針となる制御情報を保持する制御情報データベースと、

前記フィルタリング最適化手段が前記アクセスリストから最大アクセス許容数分のアクセス要求情報を読み出す際に前記アクセスリストがユーザクラス別に登録されている場合、前記制御情報データベースから抽出された制御情報に基づき前記アクセスリストの各ユーザクラスからアクセス要求情報を読み出すユーザクラス別アクセス要求読出手段を

有することを特徴とするアクセス制御サーバ。

#### 【0139】

（付記9） 付記6記載のアクセス制御サーバにおいて、

パケットフィルタリング設定情報を生成する際にアクセス要求情報に有効タイ

マを設定する有効タイマ設定手段と、

前記有効タイマの満了時にネットワーク装置に設定したパケットフィルタリング制御を解除するフィルタリング解除手段を  
有することを特徴とするアクセス制御サーバ。

【0140】

(付記10) ネットワーク装置を介してIPネットワークに接続され、ユーザにサービスを提供するサービスサーバにおいて、  
ユーザ端末とのセッションを終了したこと判定するセッション終了判定手段と

前記ユーザ端末とのセッションを終了したことをアクセス制御サーバに通知するセッション終了通知手段を  
有することを特徴とするサービスサーバ。

【0141】

(付記11) 付記3記載の受付サーバにおいて、  
前記ユーザクラス抽出手段で抽出したユーザクラスに基づき前記アクセス受付手段を介し受信したアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバにその旨を通知するユーザ認証手段を  
有することを特徴とする受付サーバ。

【0142】

(付記12) 付記6記載のアクセス制御サーバにおいて、  
付記11記載の受付サーバのユーザ認証手段からの通知に基づき前記サービスサーバにアクセス不許可とするパケットフィルタリング設定情報を生成して前記ネットワーク装置に設定するアクセス不許可フィルタリング設定手段を  
有することを特徴とするアクセス制御サーバ。

【0143】

【発明の効果】

上述の如く、請求項1に記載の発明は、受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、アクセス制御サーバは、サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求

分だけアクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うため、ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

## 【 0 1 4 4 】

請求項 2 に記載の発明は、受付サーバは、アクセス受付手段を介しユーザ端末からのアクセス要求情報を受信して保持するアクセス登録手段を有し、アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけアクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うフィルタリング最適化手段を有するため、ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

## 【 0 1 4 5 】

請求項 3 に記載の発明は、ユーザ端末からのアクセス要求情報を保持するアクセスリストと、各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロフィールと、ユーザ端末からのアクセスを受け付けるアクセス受付手段と、アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリストに受付順に登録するアクセス登録手段と、受信したアクセス要求情報から IP アドレスを抽出し、IP アドレスによりユーザを特定して前記ユーザプロフィールからユーザクラスを抽出するユーザクラス抽出手段と、アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザクラス別アクセス登録手段を有するため、ユーザクラス別にユーザからのアクセス要求情報を登録することができる。

## 【 0 1 4 6 】

請求項 4 に記載の発明は、ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位置に応じた待ち合わせを行っているユーザ数から予測

待ち合わせ時間を算出する予測待合時間算出手段と、算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を有するため、ユーザにサービスへのアクセス可能となるまでの時間を通知してユーザからのアクセス要求の待合せを可能とし、ユーザに与える負担を軽減できる。

## 【 0 1 4 7 】

請求項 5 に記載の発明は、ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するアクセス確認手段と、アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を有するため、ユーザに待合せを行うことを確認することができる。

## 【 0 1 4 8 】

付記 6 に記載の発明は、サービスサーバの処理能力に関する情報及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持するアクセス情報データベースと、ネットワーク装置を制御するトラヒック制御手段と、サービスサーバの処理能力に関する情報に基づき最大アクセス許容数を算出する静的アクセス許容数算出手段と、受付サーバでユーザ端末からのアクセス要求情報を保持するアクセスリストの先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバにアクセス可能とするパケットフィルタリング設定情報を生成し前記トラヒック制御手段を介して前記ネットワーク装置に設定するフィルタリング最適化手段を有するため、サービスサーバの処理能力に見合うユーザからのアクセスを受け付ける制御を行うことができる。

## 【 0 1 4 9 】

付記 7 に記載の発明は、サービスサーバの負荷状態及びサービスサーバを収容するネットワーク装置のトラフィック状態を監視する負荷・トラヒック監視装置と、周期的に負荷・トラヒック監視装置と通信して前記負荷状態及びトラヒック状態の情報を抽出して前記アクセス情報データベースの最大アクセス許容数を算出すると共に、算出した最大アクセス許容数を前記アクセス情報データベースに



登録する動的アクセス許容数算出手段を有するため、サービスサーバの負荷状況やトラフィック状況に応じてサービスサーバが最適に動作可能なアクセス分のユーザにアクセスを許可することが可能となる。

## 【 0 1 5 0 】

付記 8 に記載の発明は、ユーザ端末からのアクセス要求情報を前記アクセスリストから読み出す際に読み出す指針となる制御情報を保持する制御情報データベースと、フィルタリング最適化手段が前記アクセスリストから最大アクセス許容数分のアクセス要求情報を読み出す際に前記アクセスリストがユーザクラス別に登録されている場合、前記制御情報データベースから抽出された制御情報に基づき前記アクセスリストの各ユーザクラスからアクセス要求情報を読み出すユーザクラス別アクセス要求読出手段を有するため、ユーザクラスに応じて読み出すアクセス要求情報数を可変することができる。

## 【 0 1 5 1 】

付記 9 に記載の発明は、パケットフィルタリング設定情報を生成する際にアクセス要求情報に有効タイマを設定する有効タイマ設定手段と、有効タイマの満了時にネットワーク装置に設定したパケットフィルタリング制御を解除するフィルタリング解除手段を有するため、有効タイマを用いて各アクセスの時間管理を行い、アクセス許可を解除することができる。

## 【 0 1 5 2 】

付記 1 0 に記載の発明は、ユーザ端末とのセッションを終了したこと判定するセッション終了判定手段と、ユーザ端末とのセッションを終了したことをアクセス制御サーバに通知するセッション終了通知手段を有するため、セッションが終了したアクセスのアクセス許可を解除することができる。

## 【 0 1 5 3 】

付記 1 1 に記載の発明は、ユーザクラス抽出手段で抽出したユーザクラスに基づき前記アクセス受付手段を介し受信したアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバにその旨を通知するユーザ認証手段を有し、また、付記 1 2 に記載の発明は、受付サーバのユーザ認証手段からの通知に基づき前記サービスサーバにアクセス不許可とするパケットフ

フィルタリング設定情報を生成して前記ネットワーク装置に設定するアクセス不許可フィルタリング設定手段を有するため、ユーザがアクセス権限を持っている場合にのみサービスサーバのアクセスを許可することができる。

【図面の簡単な説明】

【図 1】

本発明方法の一実施例の全体構成図である。

【図 2】

本発明方法のパケットフィルタリング機能を説明するための図である。

【図 3】

本発明方法の予測待合時間通知機能を説明するための図である。

【図 4】

本発明方法の予測待合時間通知機能を説明するための図である。

【図 5】

本発明方法の動的アクセス許容数算出機能を説明するための図である。

【図 6】

本発明方法のユーザクラス別アクセス要求読出機能を説明するための図である。

【図 7】

本発明方法の有効タイマ機能を説明するための図である。

【図 8】

本発明方法のセッション終了機能を説明するための図である。

【図 9】

本発明方法のアクセス不許可機能を説明するための図である。

【図 10】

インターネットサービスプロバイダが受付代行サービスを行う実施例のシステム構成図である。

【図 11】

ユーザプロファイル 111 のデータ構造を示す図である。

【図 12】

アクセス情報DB 2 0 9 のデータ構造を示す図である。

【図 1 3】

アクセスリスト 1 0 9 のデータ構造を示す図である。

【図 1 4】

制御情報DB 2 1 1 を示す図である。

【図 1 5】

静的アクセス許容数算出手段 2 0 6 が実行する処理のフローチャートである。

【図 1 6】

アクセス要求情報のメッセージ構造を示す図である。

【図 1 7】

アクセス登録手段 1 0 3 の処理を詳細に説明するためのフローチャートである。

【図 1 8】

アクセス登録手段 1 0 3 の処理を詳細に説明するためのフローチャートである。

【図 1 9】

フィルタリング要求のメッセージ構造を示す図である。

【図 2 0】

フィルタリング最適化手段 2 0 4 の処理を詳細に説明するためのフローチャートである。

【図 2 1】

フィルタリング最適化手段 2 0 4 の処理を詳細に説明するためのフローチャートである。

【図 2 2】

フィルタリング・コマンド実行要求のメッセージ構造を示す図である。

【図 2 3】

トラヒック制御手段 2 1 0 の処理を詳細に説明するためのフローチャートである。

【図 2 4】

有効タイマ設定手段 2 0 3 の処理を詳細に説明するためのフローチャートである。

【図 2 5】

フィルタリング解除手段 2 0 2 の処理を詳細に説明するためのフローチャートである。

【図 2 6】

セッション終了通知手段 3 0 1 の処理を詳細に説明するためのフローチャートである。

【図 2 7】

セッション終了通知のメッセージ構造を示す図である。

【図 2 8】

セッション完了フィルタリング解除手段 2 0 8 の処理を詳細に説明するためのフローチャートである。

【図 2 9】

アクセス確認手段 1 0 4 の処理を詳細に説明するためのフローチャートである。

【図 3 0】

待合せ確認通知手段 1 0 5 の処理を詳細に説明するためのフローチャートである。

【図 3 1】

予測待合時間算出手段 1 0 6 の処理を詳細に説明するためのフローチャートである。

【図 3 2】

アクセス情報通知手段 1 0 7 の処理を詳細に説明するためのフローチャートである。

【図 3 3】

動的アクセス許容数算出手段 2 0 7 の処理を詳細に説明するためのフローチャートである。

【図 3 4】

ユーザクラス別アクセス登録手段 1 0 8 の処理を詳細に説明するためのフローチャートである。

【図 3 5】

ユーザクラス抽出手段 1 0 2 の処理を詳細に説明するための図である。

【図 3 6】

ユーザクラス別アクセス要求読出手段 2 0 5 の処理を詳細に説明するためのフローチャートである。

【図 3 7】

有効タイマ設定要求のメッセージ構造を示す図である。

【図 3 8】

ユーザ認証手段 1 0 1 の処理を詳細に説明するためのフローチャートである。

【図 3 9】

アクセス不許可フィルタリング設定手段 2 0 1 の処理を詳細に説明するためのフローチャートである。

【符号の説明】

- 1 0    コアネットワーク
- 2 0, 3 0, 4 0    ネットワーク装置
- 5 0    ユーザ端末
- 1 0 0    受付サーバ
- 3 0 0    サービスサーバ
- 1 0 2    ユーザクラス抽出手段
- 1 0 3    アクセス登録手段
- 1 0 4    アクセス確認手段
- 1 0 5    待合せ確認通知手段
- 1 0 6    予測待合時間算出手段
- 1 0 7    アクセス情報通知手段
- 1 0 8    ユーザクラス別アクセス登録手段
- 1 0 9    アクセスリスト
- 1 1 0    アクセス受付手段

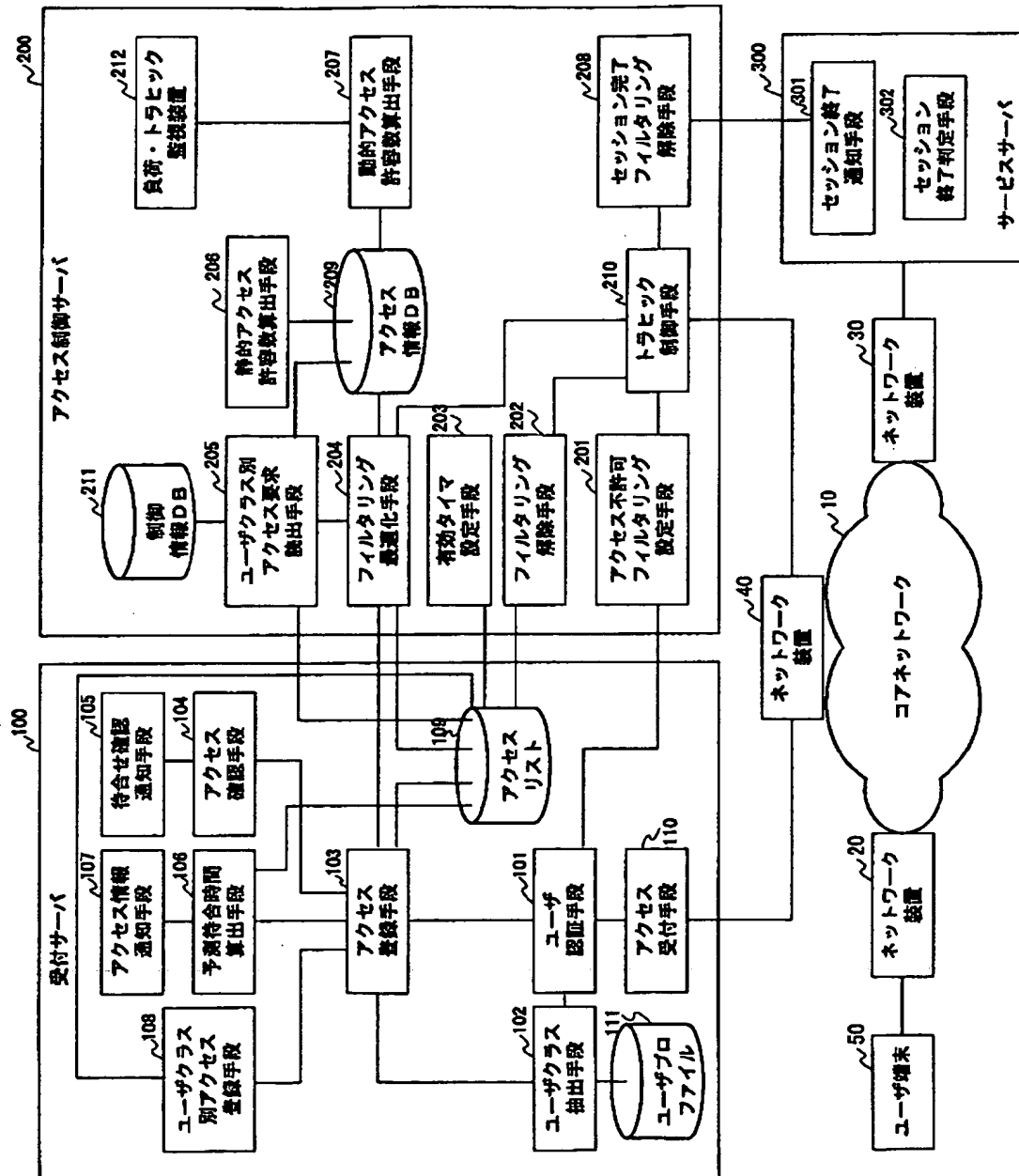
- 1 1 1 ユーザプロフィール
- 2 0 0 アクセス制御サーバ
- 2 0 1 アクセス不許可フィルタリング設定手段
- 2 0 2 フィルタリング解除手段
- 2 0 3 有効タイマ設定手段
- 2 0 4 フィルタリング最適化手段
- 2 0 5 ユーザクラス別アクセス要求読出手段
- 2 0 6 静的アクセス許容数算出手段
- 2 0 7 動的アクセス許容数算出手段
- 2 0 8 セッション完了フィルタリング解除手段
- 2 0 9 アクセス情報 D B
- 2 1 0 トラヒック制御手段
- 2 1 1 制御情報 D B
- 2 1 2 負荷・トラヒック監視装置
- 3 0 1 セッション終了通知手段
- 3 0 2 セッション終了判定手段

【書類名】

凶面

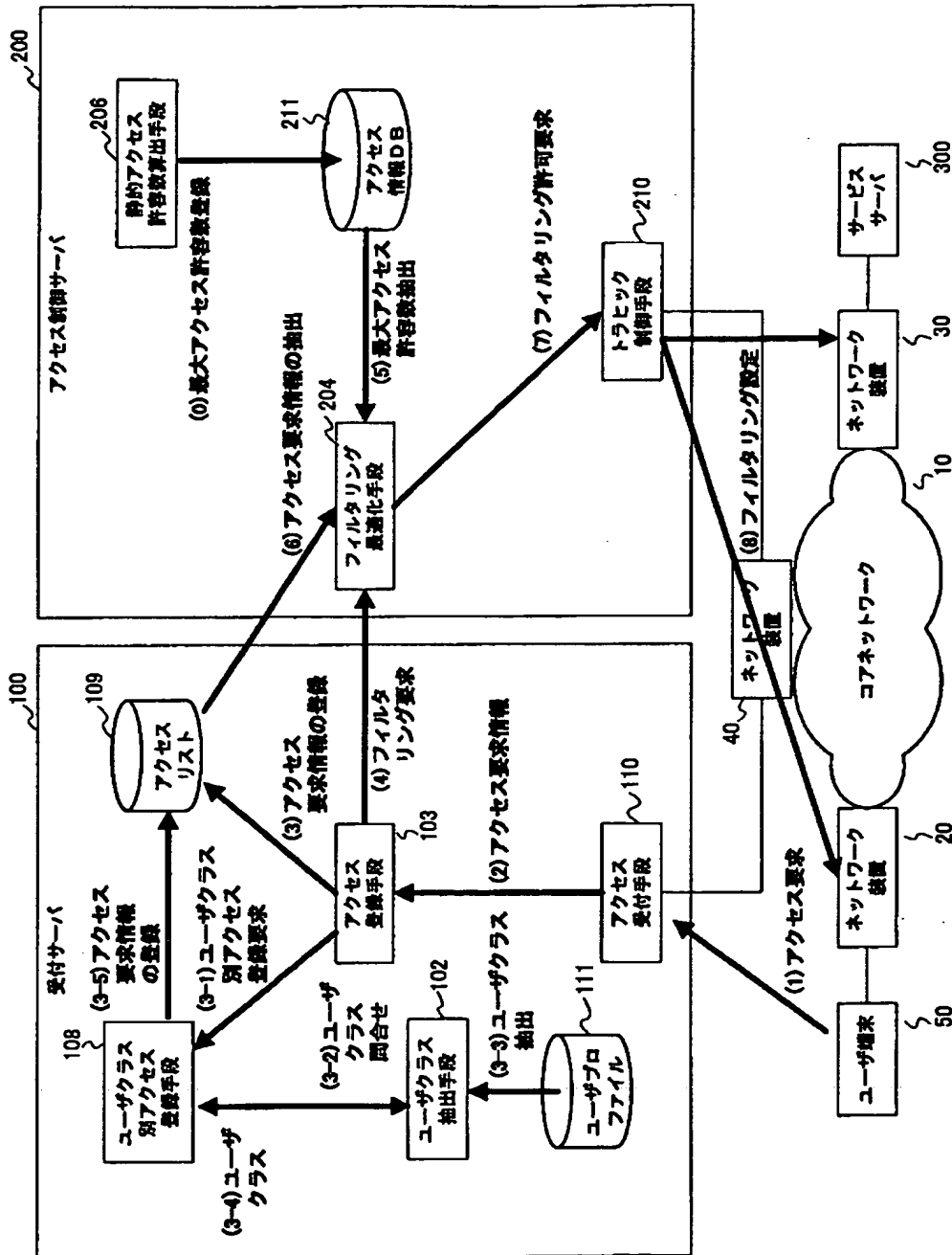
【図 1】

## 本発明方法の一実施例の全体構成図



【図 2】

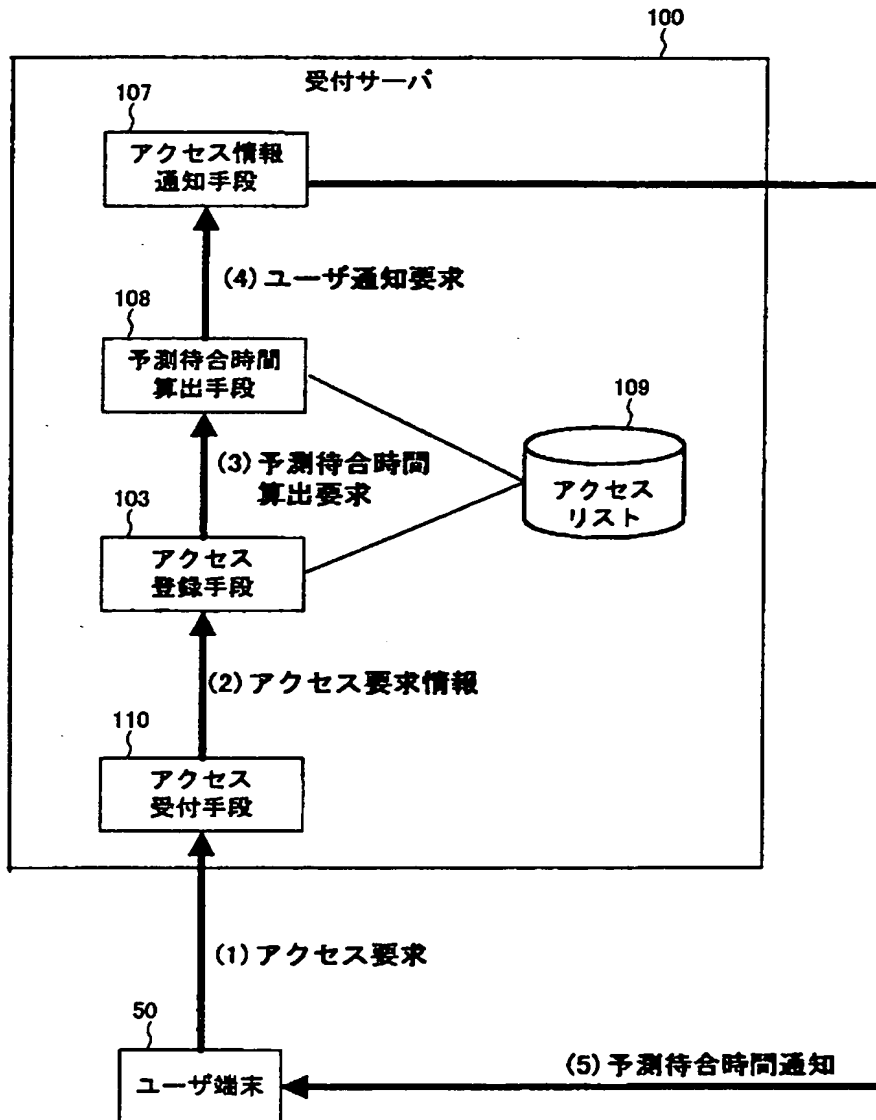
本発明方法のパケットフィルタリング機能を説明するための図





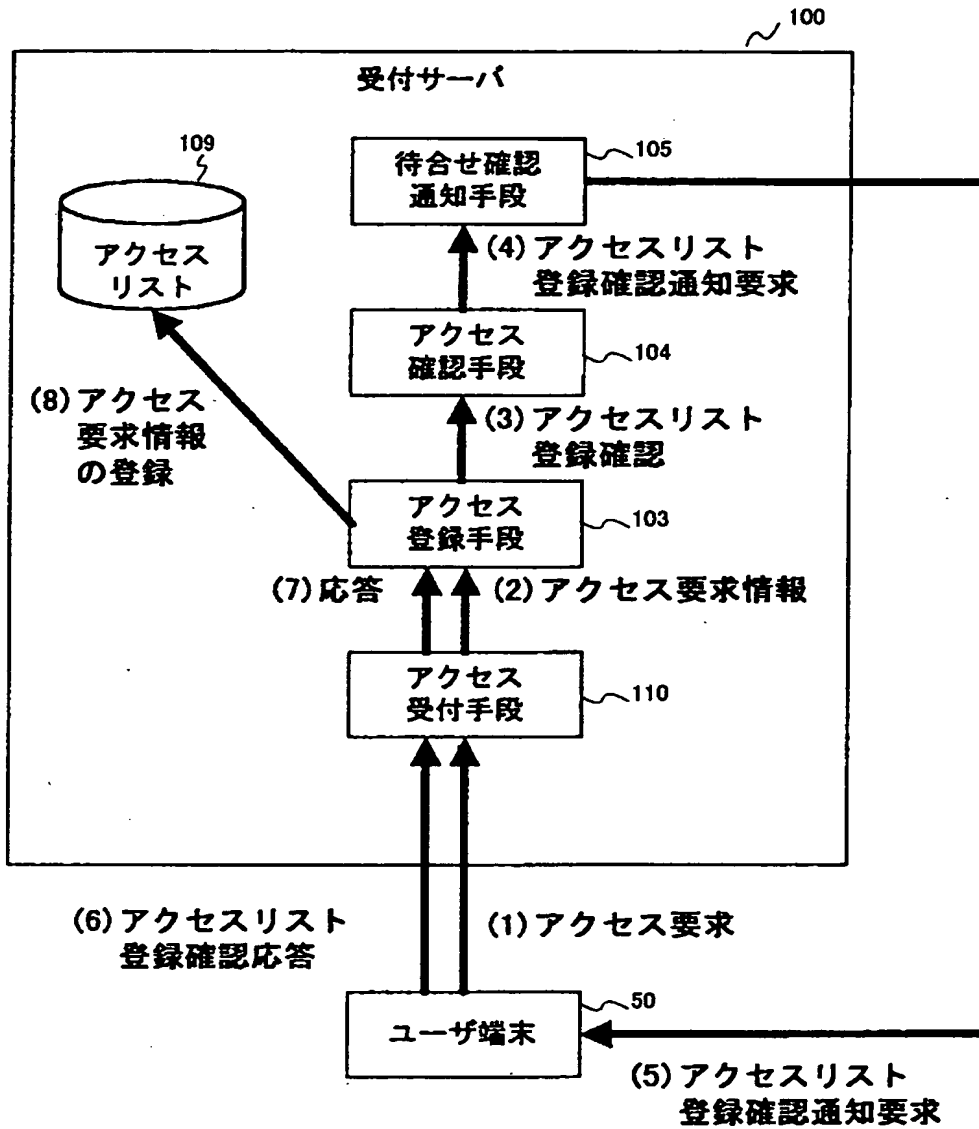
【図 3】

本発明方法の予測待合時間通知機能を説明するための図



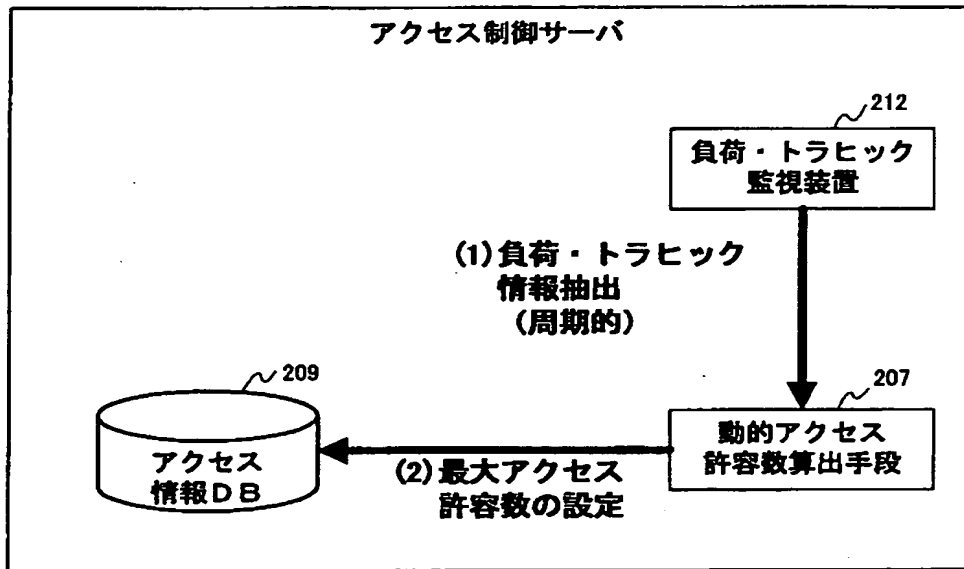
【図 4】

本発明方法の予測待合時間通知機能を説明するための図



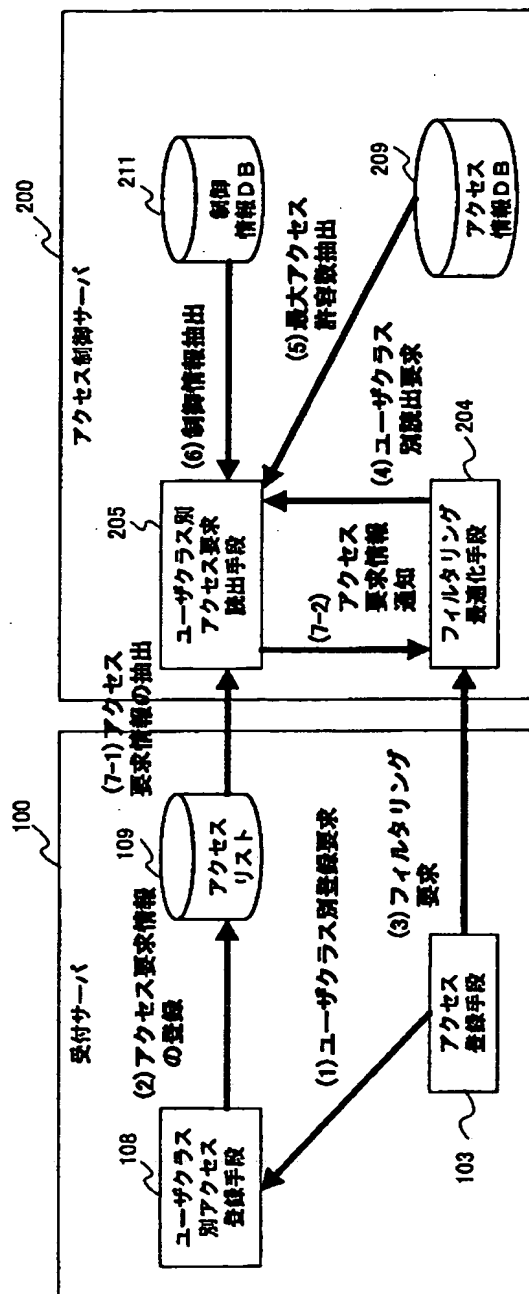
【図 5】

本発明方法の動的アクセス許容数算出機能を説明するための図



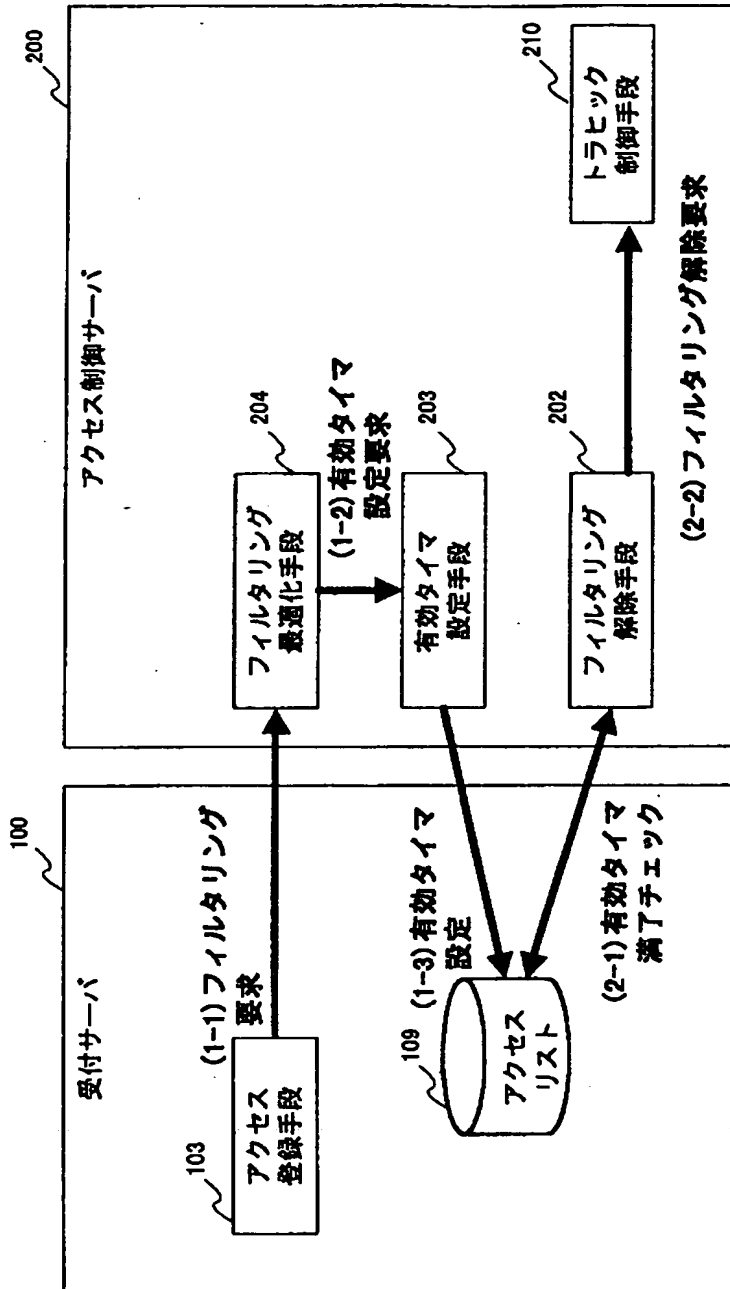
【図 6】

本発明方法のユーザクラス別アクセス要求読出機能を説明するための図



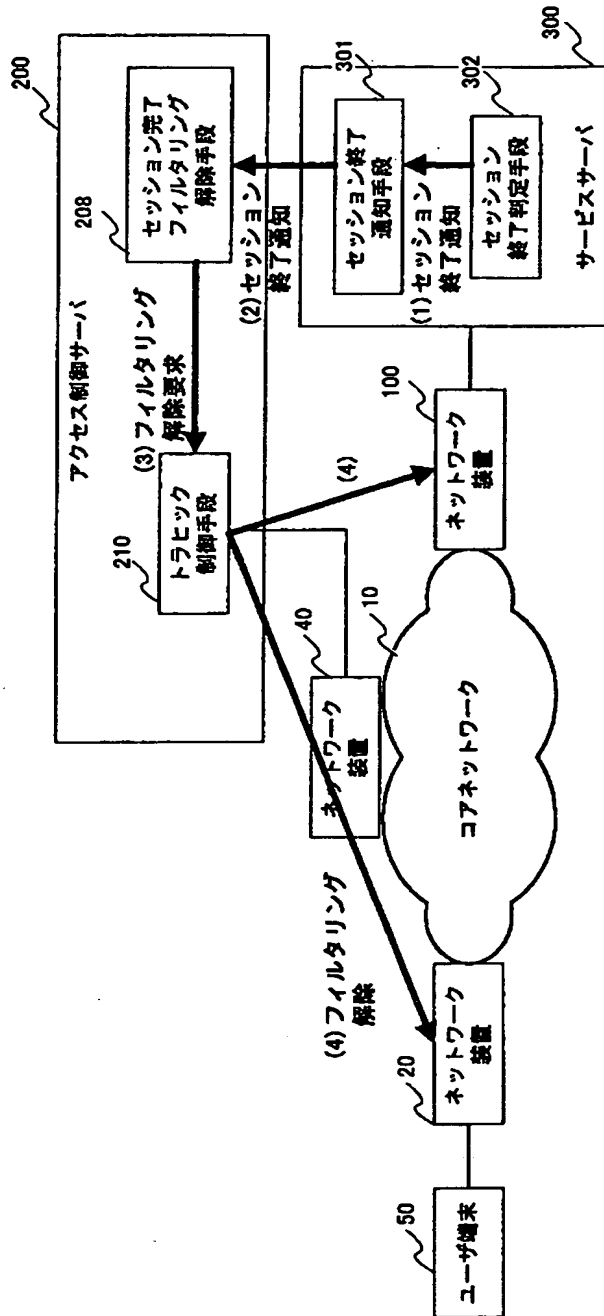
【図 7】

本発明方法の有効タイマ機能を説明するための図



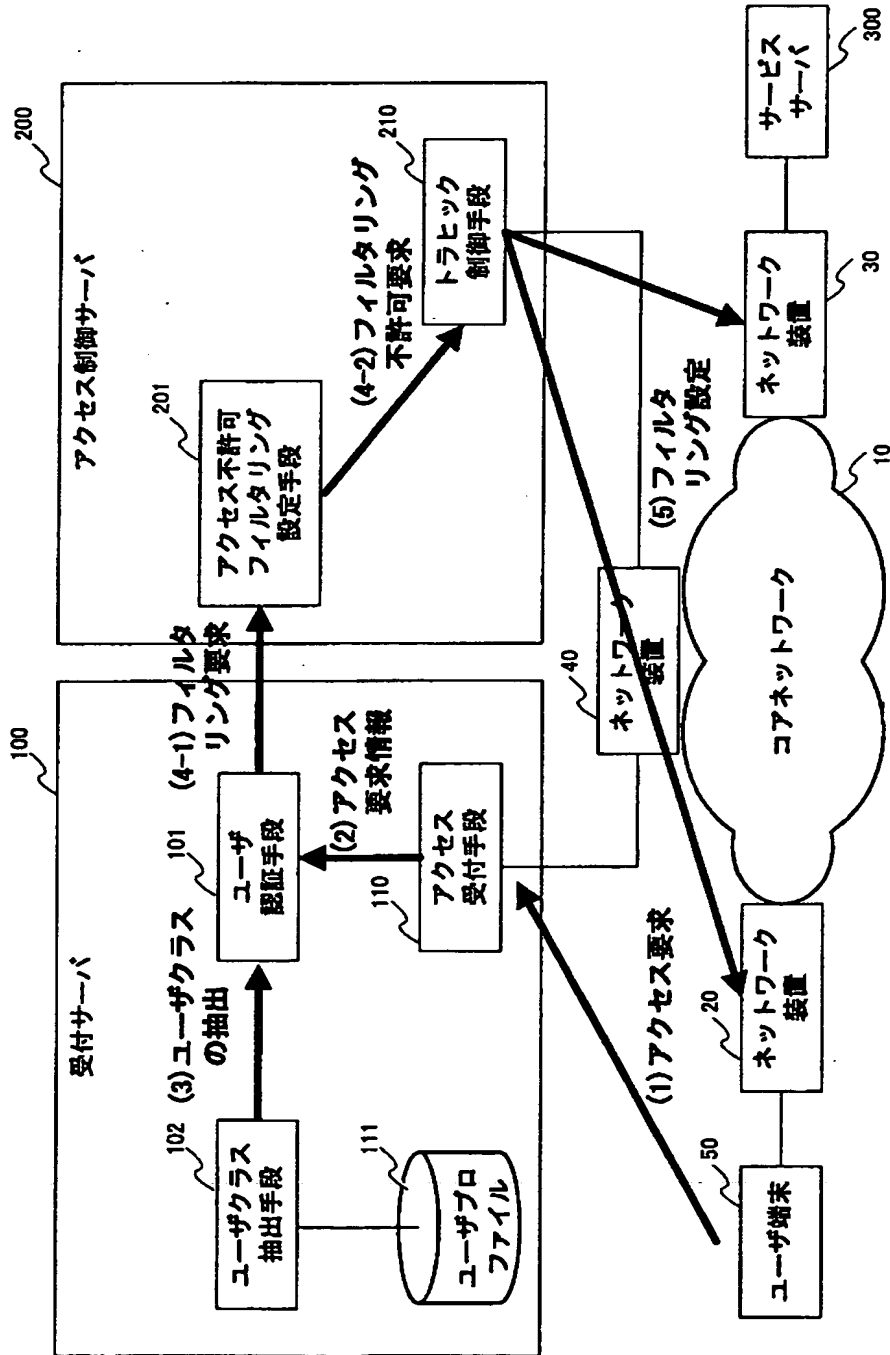
【図 8】

本発明方法のセッション終了機能を説明するための図



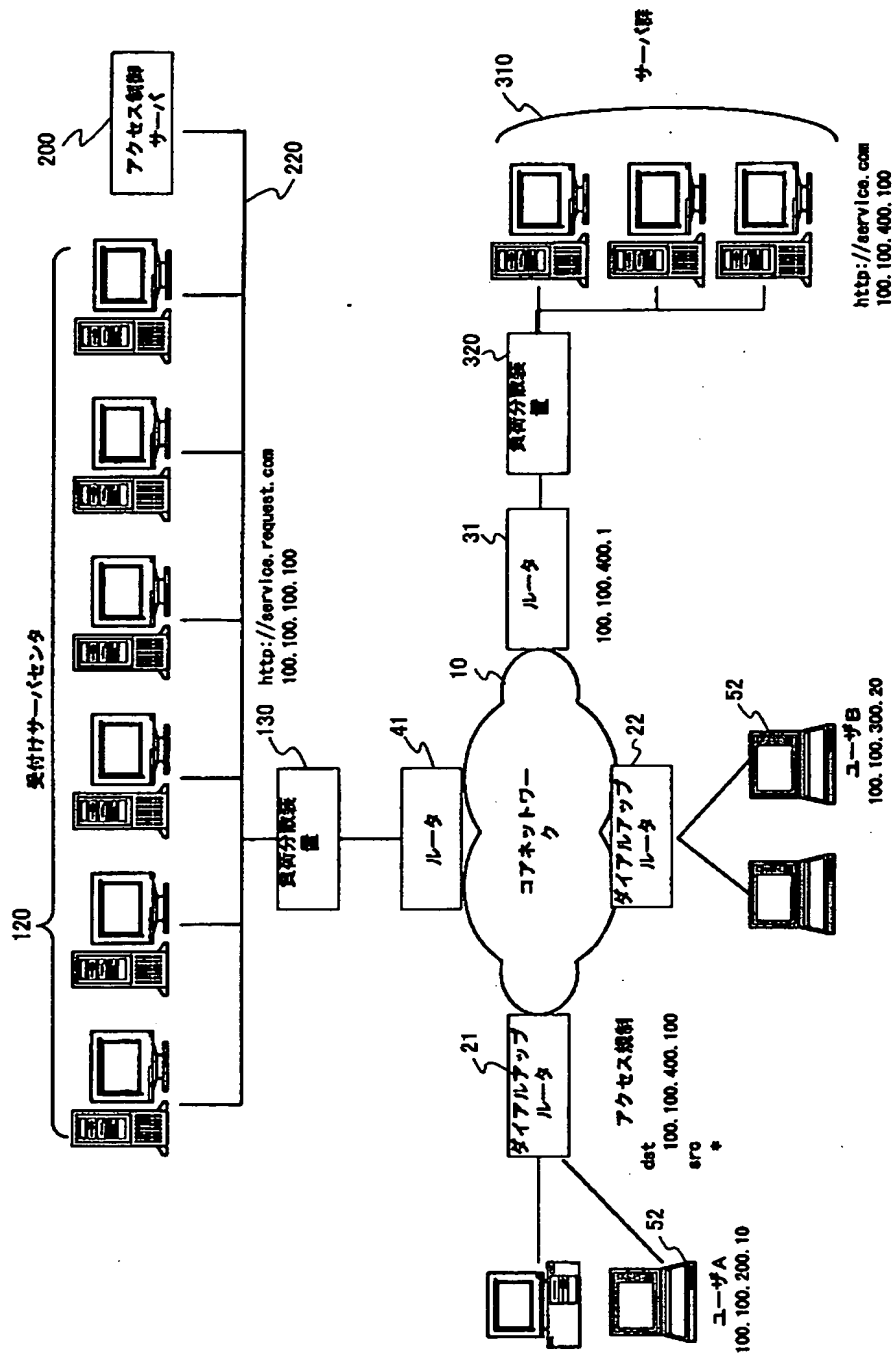
【図 9】

本発明方法のアクセス不許可機能を説明するための図



【図 10】

## インターネットサービスプロバイダが 受付代行サービスを行う実施例のシステム構成図





【図 1 1】

ユーザプロフィール111のデータ構造を示す図

ユーザプロフィール

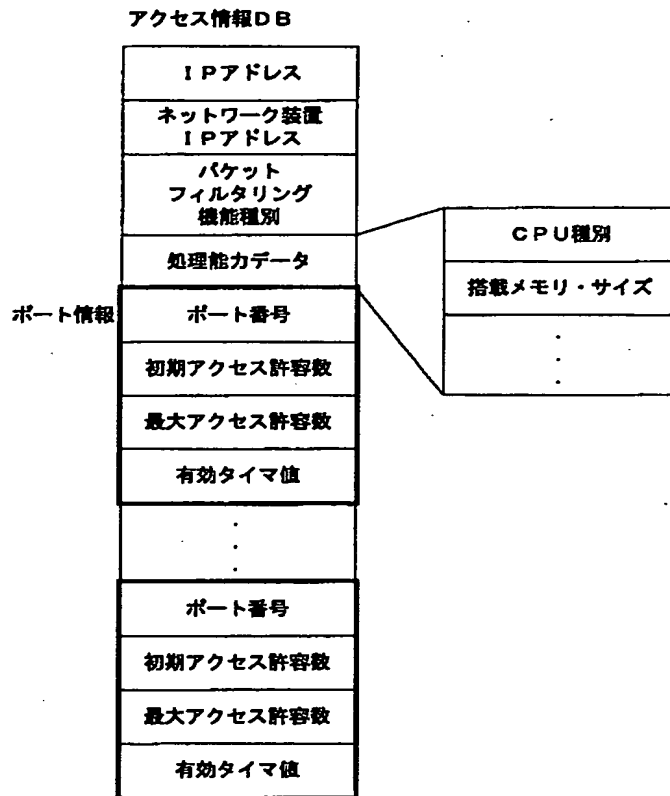
送信元IPアドレス
送信先IPアドレス
送信先ポート番号
ユーザクラス
.
.
.
送信先IPアドレス
送信先ポート番号
ユーザクラス

ユーザクラス：

- 1→高優先
- 2→中優先
- 3→低優先
- 0→不許可

【図 1 2】

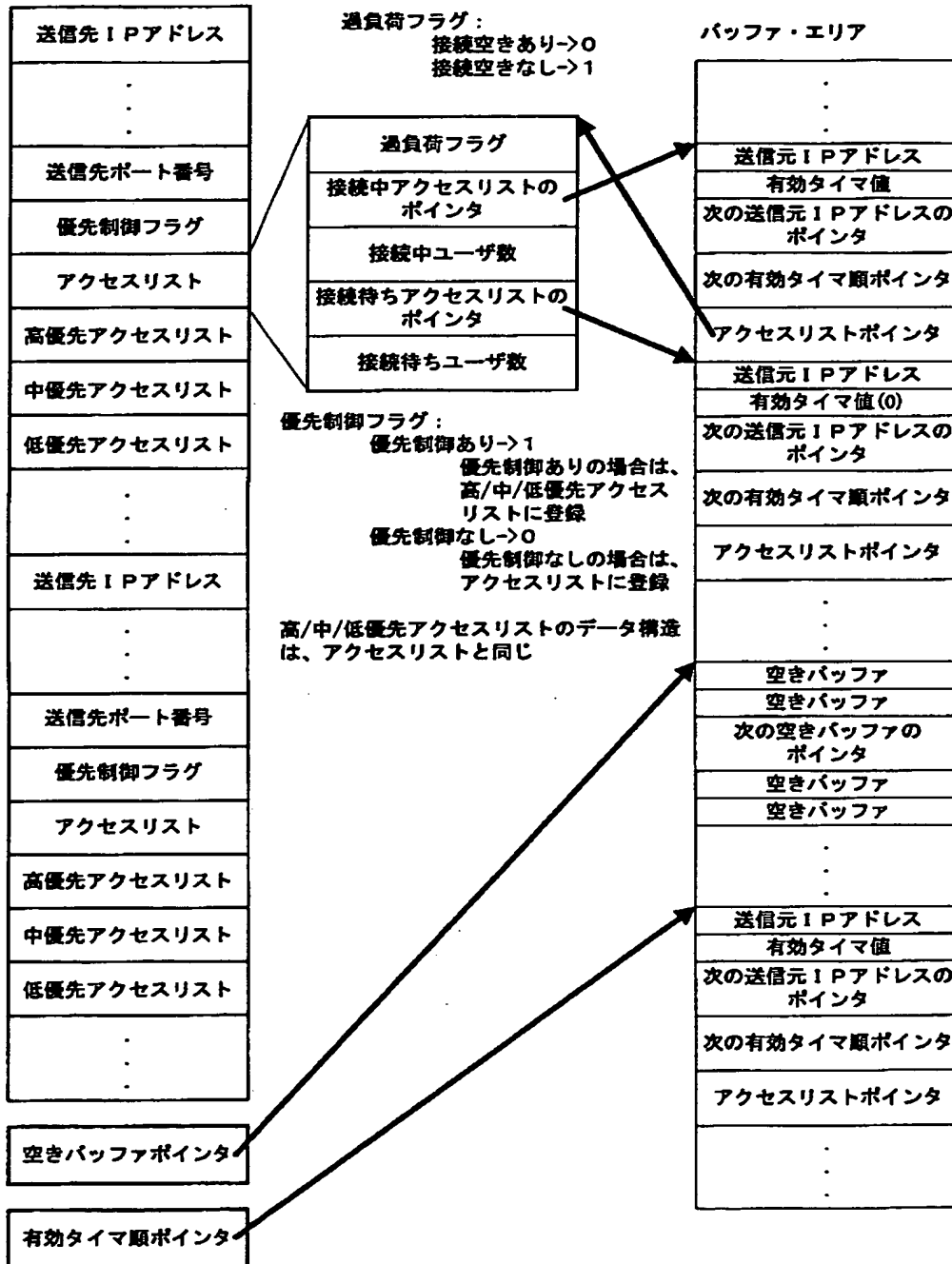
アクセス情報DB209のデータ構造を示す図



【図 13】

## アクセスリスト109のデータ構造を示す図

アクセスリスト



【図 14】

制御情報DB211を示す図

制御情報DB

ユーザクラス数
・ ・ ・
読出制御データ
・ ・ ・

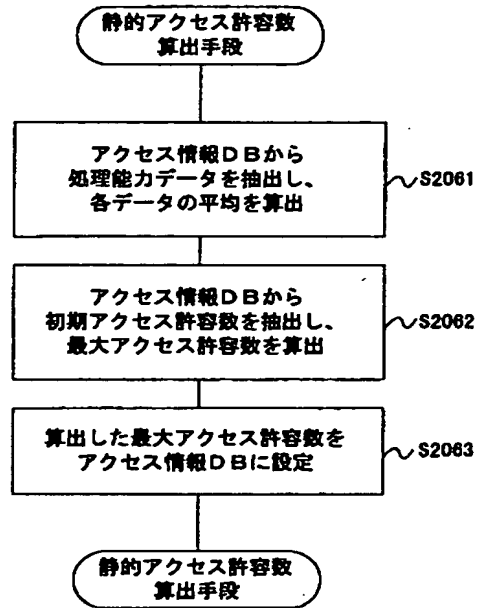
ユーザクラス数：  
高優先クラス、中優先クラス、  
低優先クラスの場合は、3

IPアドレス
・ ・ ・
ポート番号
読出比率
・ ・ ・

読出比率：  
高優先クラス、中優先クラス、  
低優先クラスの読み出し比率が  
3：2：1なら321というデータ  
が設定されている。

【図 1 5】

静的アクセス許容数算出手段206が実行する処理のフローチャート図



【図 1 6】

アクセス要求情報のメッセージ構造を示す図

アクセス要求情報

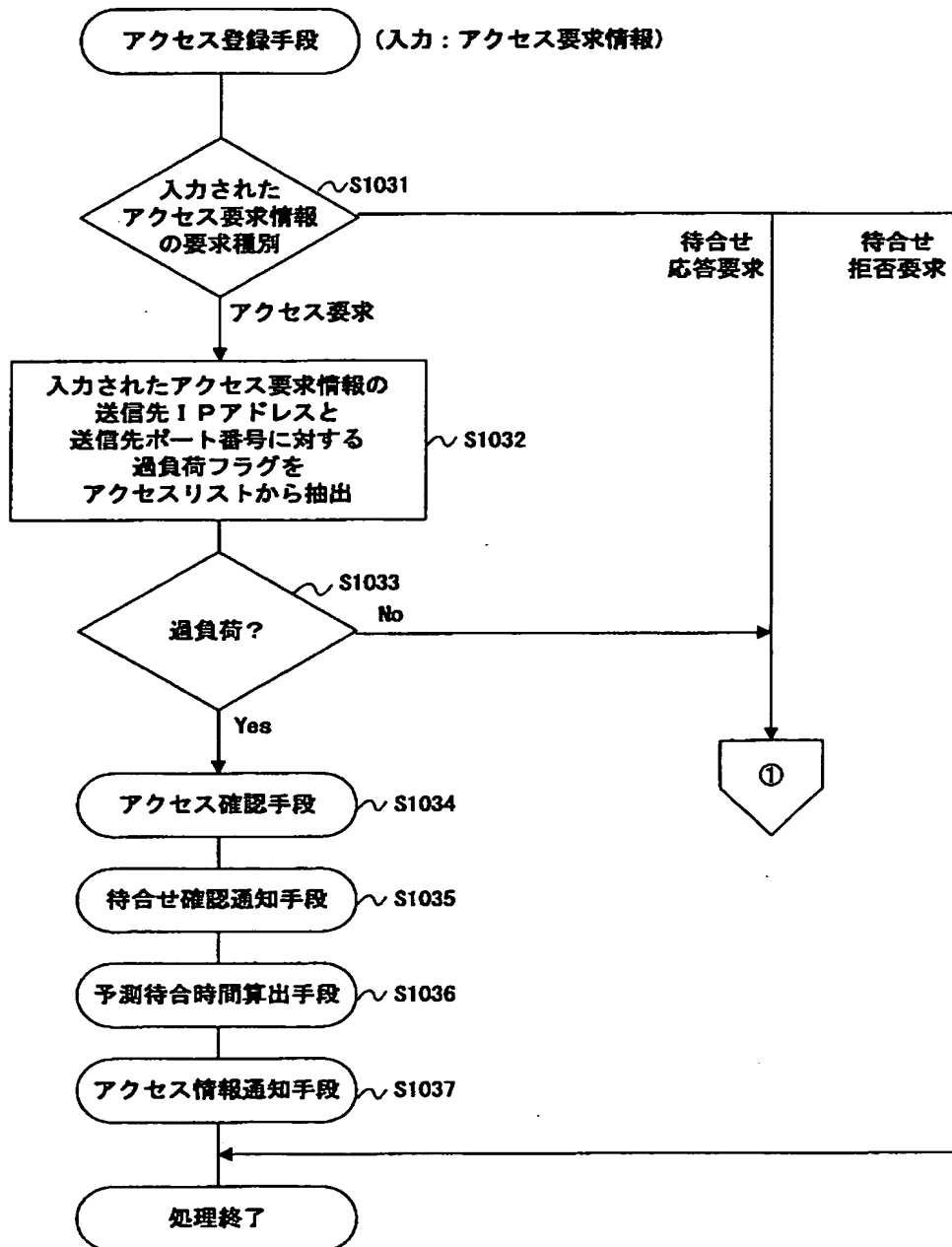
要求種別
送信元 I P アドレス
送信先 I P アドレス
送信先ポート番号

要求種別：

アクセス要求->0  
 待合せ応答要求->1  
 待合せ拒否要求->2

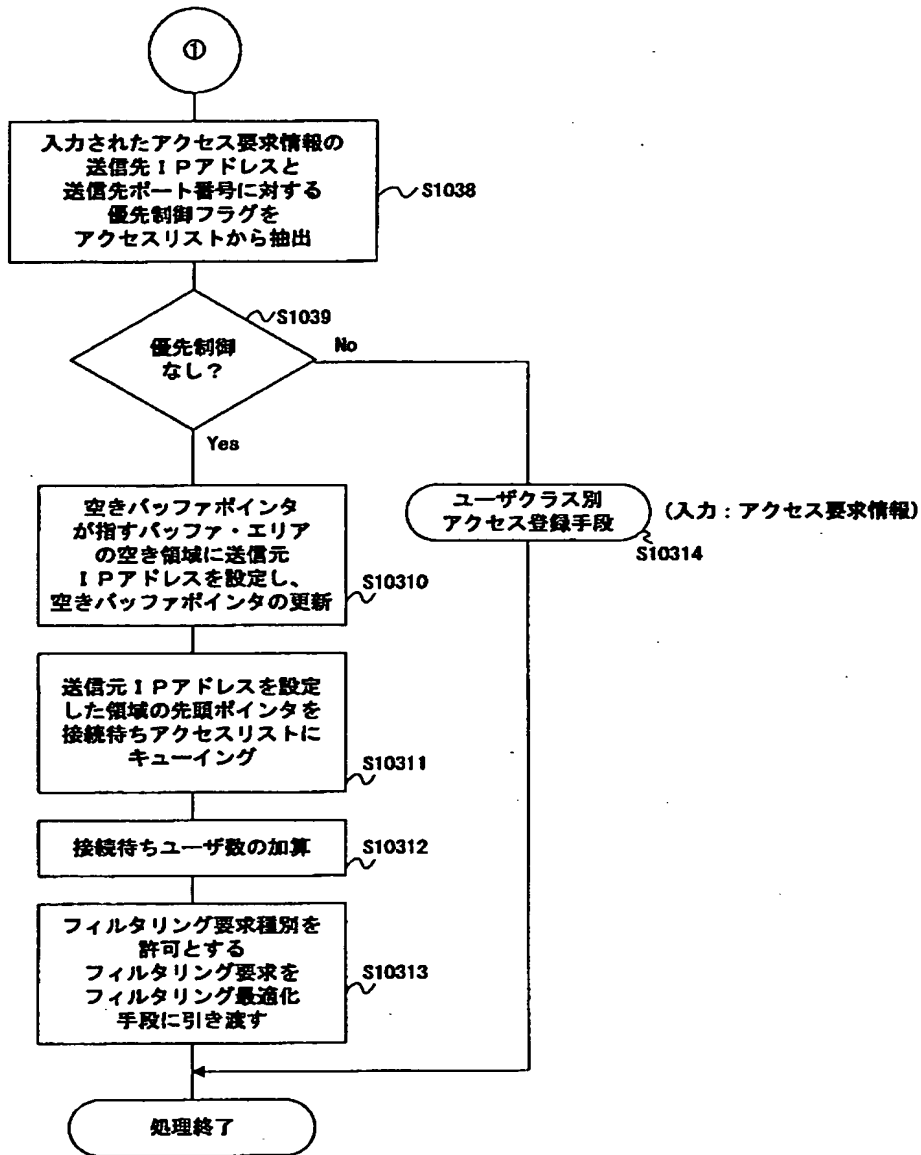
【図 1 7】

アクセス登録手段103の処理を詳細に説明するためのフローチャート



【図 1 8】

アクセス登録手段103の処理を詳細に説明するためのフローチャート





【図 19】

フィルタリング要求のメッセージ構造を示す図

フィルタリング要求

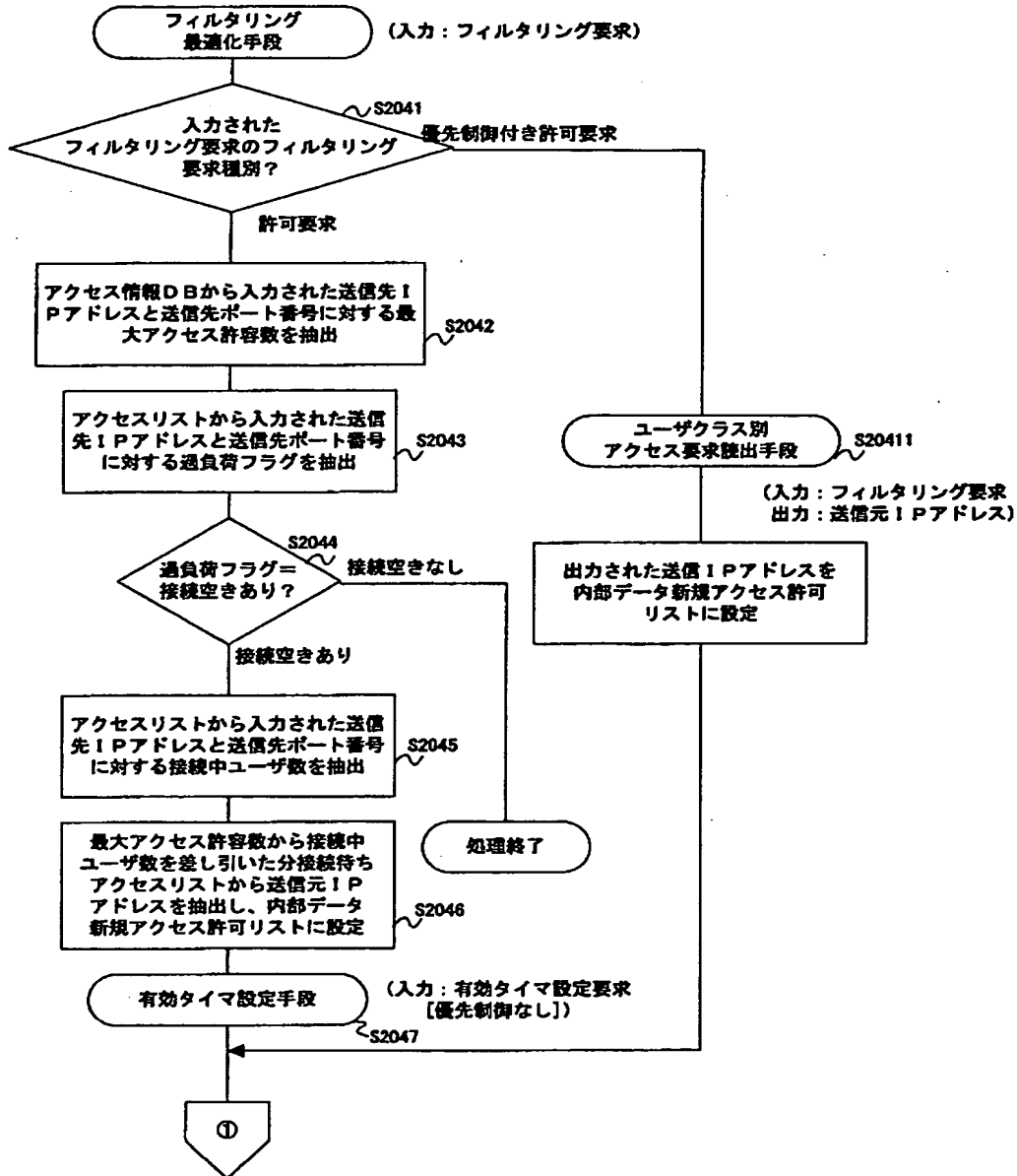
フィルタリング要求種別
送信元 IP アドレス
送信先 IP アドレス
送信先ポート番号

フィルタリング要求種別：

- 0：許可要求
- 1：不許可要求
- 2：優先制御付き許可要求
- 3：（許可）解除要求

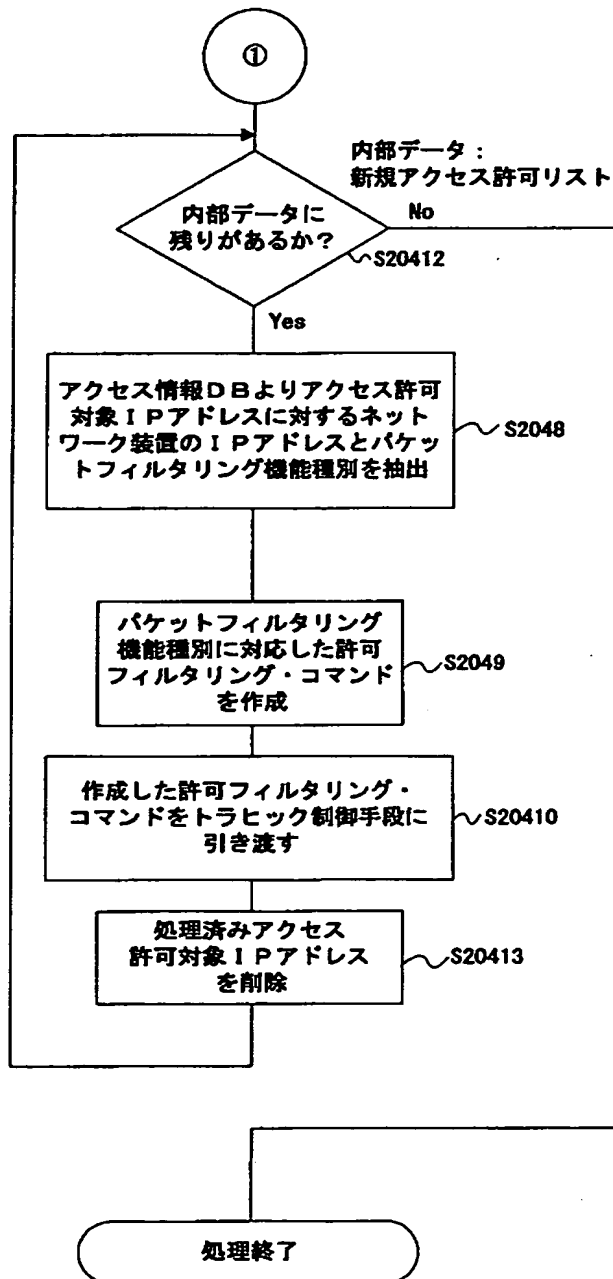
【図 20】

フィルタリング最適化手段204の処理を詳細に説明するためのフローチャート



【図 21】

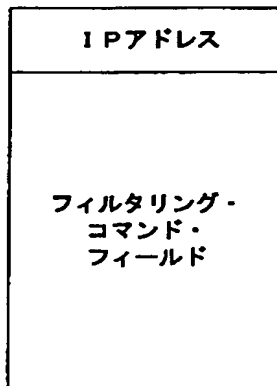
フィルタリング最適化手段204の処理を詳細に説明するためのフローチャート



【図 2 2】

フィルタリング・コマンド実行要求のメッセージ構造を示す図

フィルタリング・コマンド  
実行要求

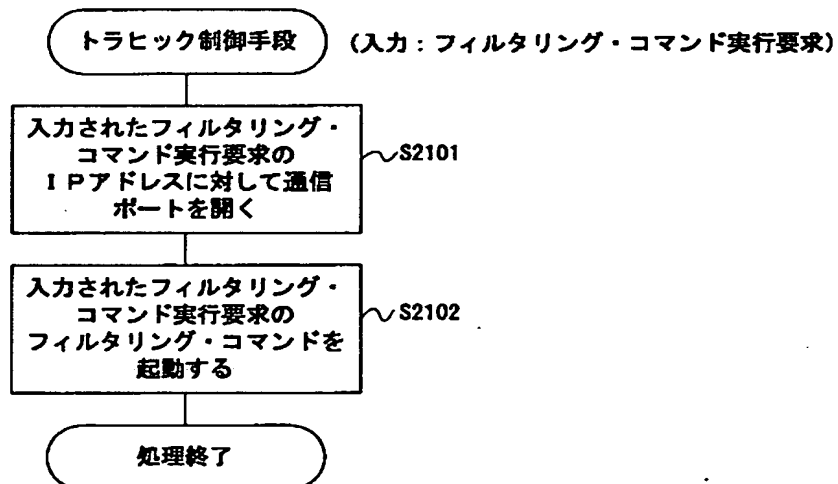


IPアドレス：  
ネットワーク装置のIPアドレス

フィルタリング・コマンド・フィールド：  
各ネットワーク装置が持つパケット  
フィルタリング機能に対応する  
フィルタリング・コマンド

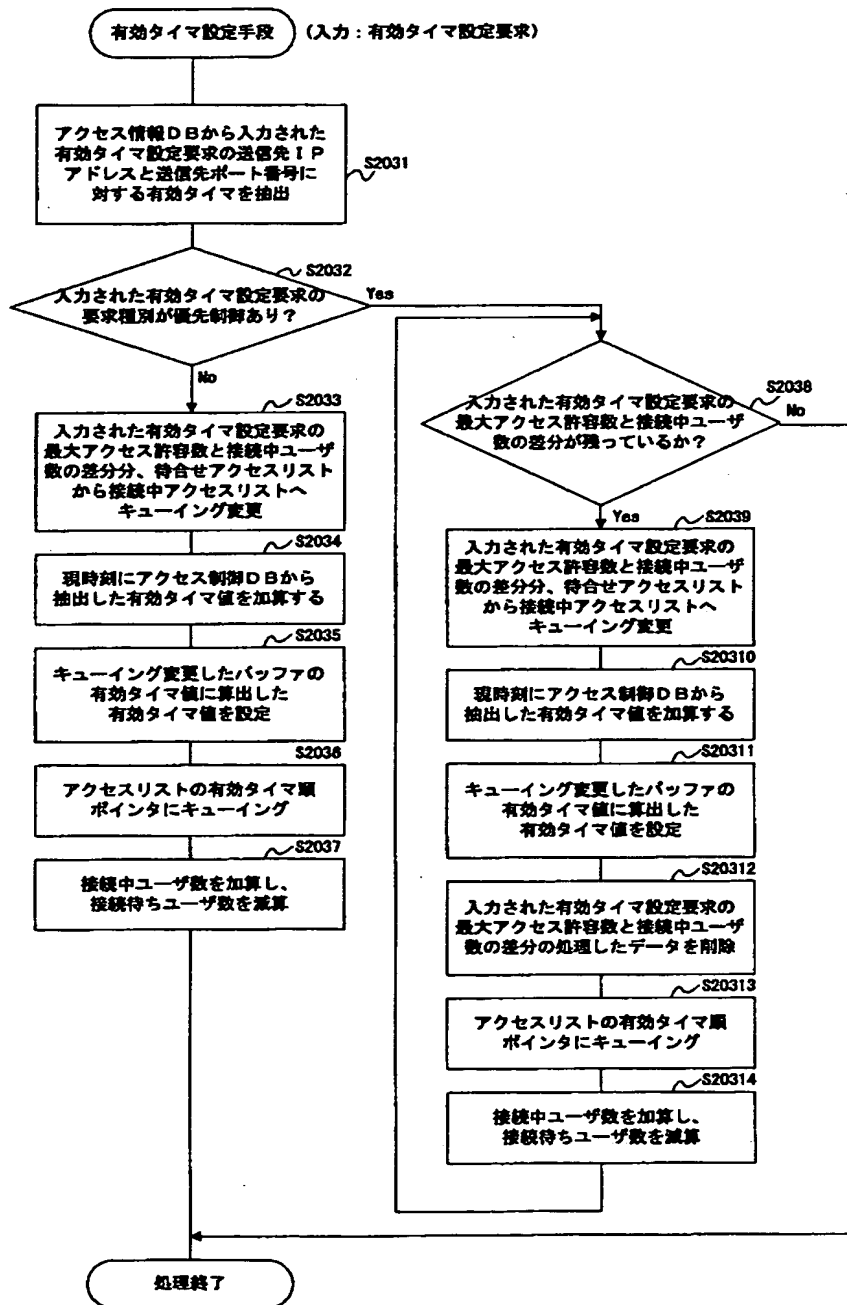
【図 2 3】

トラヒック制御手段210の処理を詳細に説明するためのフローチャート



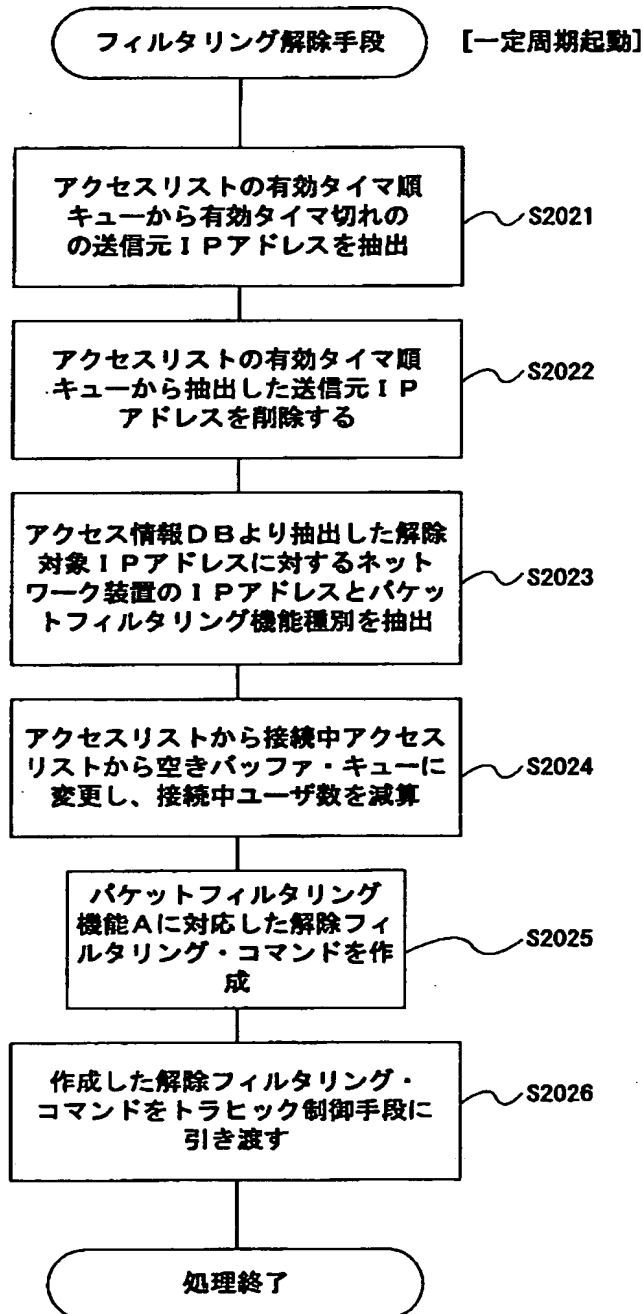
【図 24】

有効タイム設定手段203の処理を詳細に説明するためのフローチャート



【図 25】

フィルタリング解除手段202の処理を詳細に説明するためのフローチャート



【図 2 6】

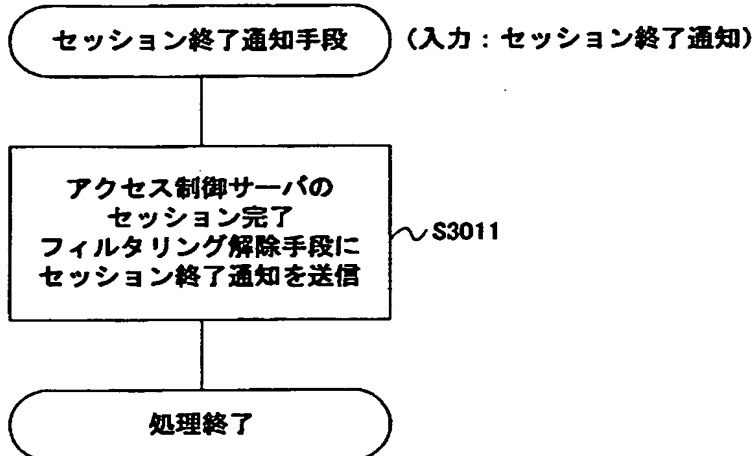
セッション終了通知手段301の処理を詳細に説明するためのフローチャート

セッション終了通知

サービスサーバ IPアドレス
サービスサーバ ポート番号
クライアント IPアドレス

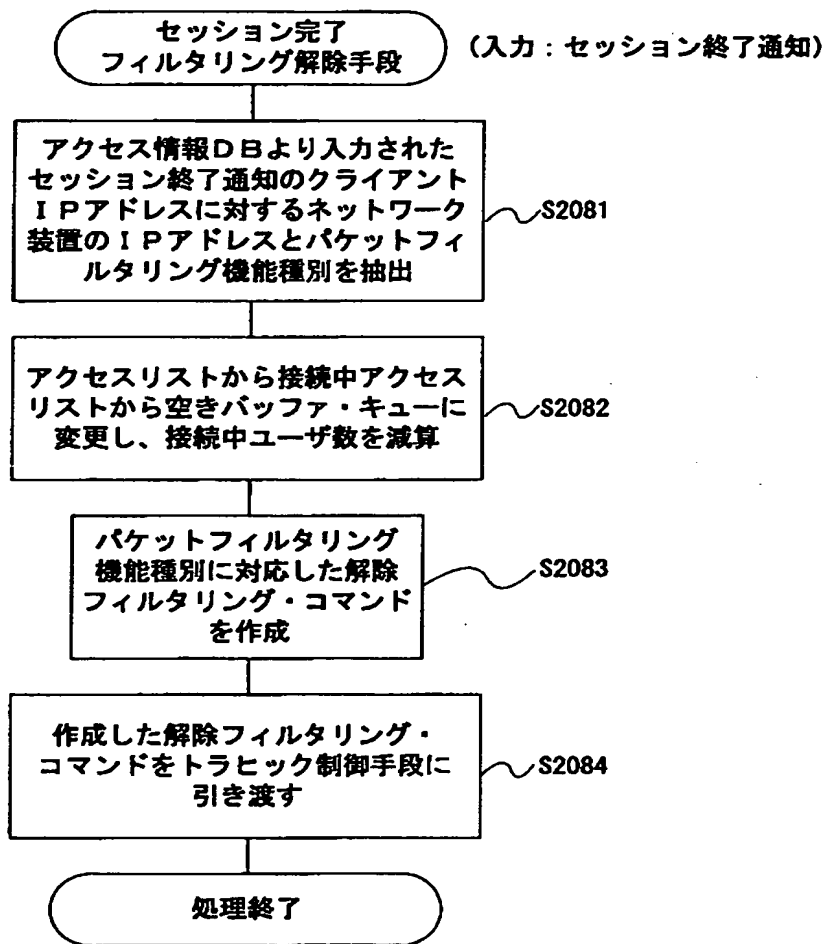
【図 2 7】

セッション終了通知のメッセージ構造を示す図



【図 2 8】

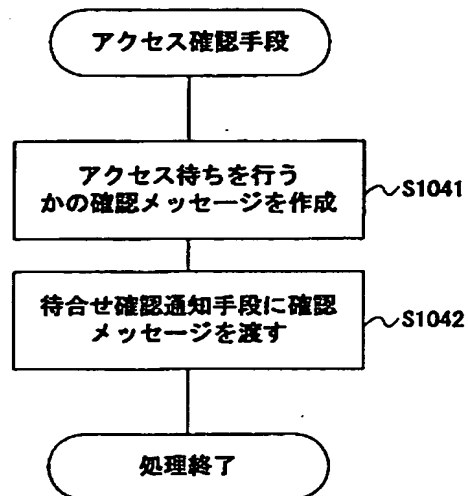
セッション完了フィルタリング解除手段208の処理を  
詳細に説明するためのフローチャート





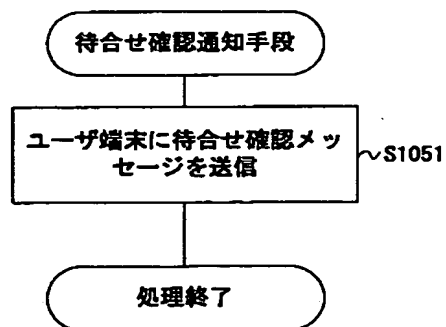
【図 2 9】

アクセス確認手段104の処理を詳細に説明するためのフローチャート



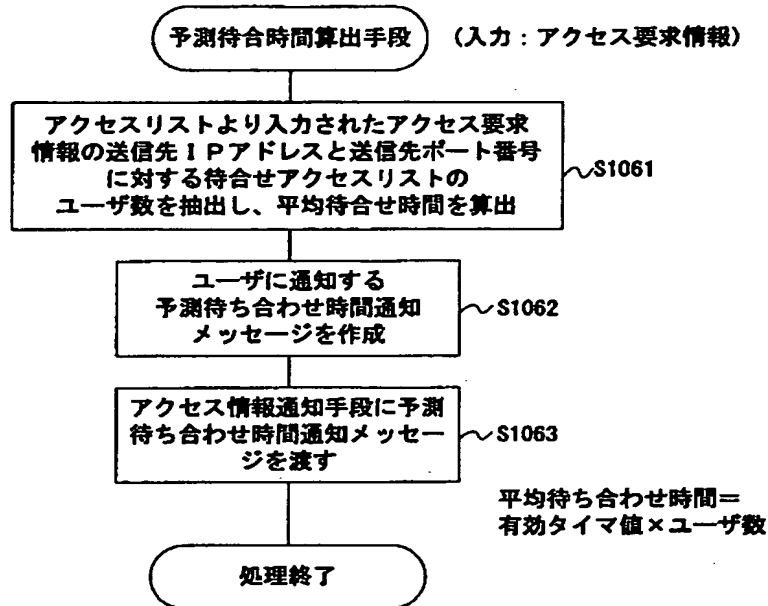
【図 3 0】

待合せ確認通知手段105の処理を詳細に説明するためのフローチャート



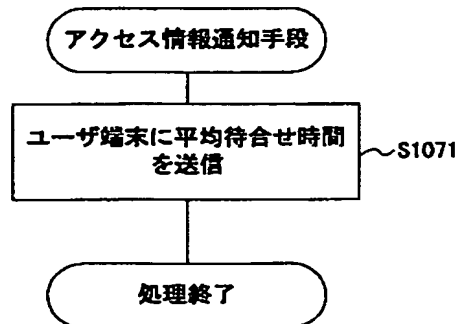
【図 3 1】

予測待ち時間算出手段106の処理を詳細に説明するためのフローチャート



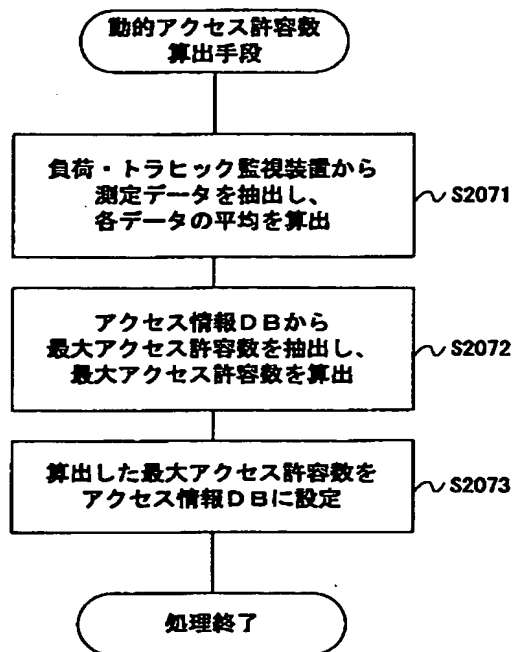
【図 3 2】

アクセス情報通知手段107の処理を詳細に説明するためのフローチャート



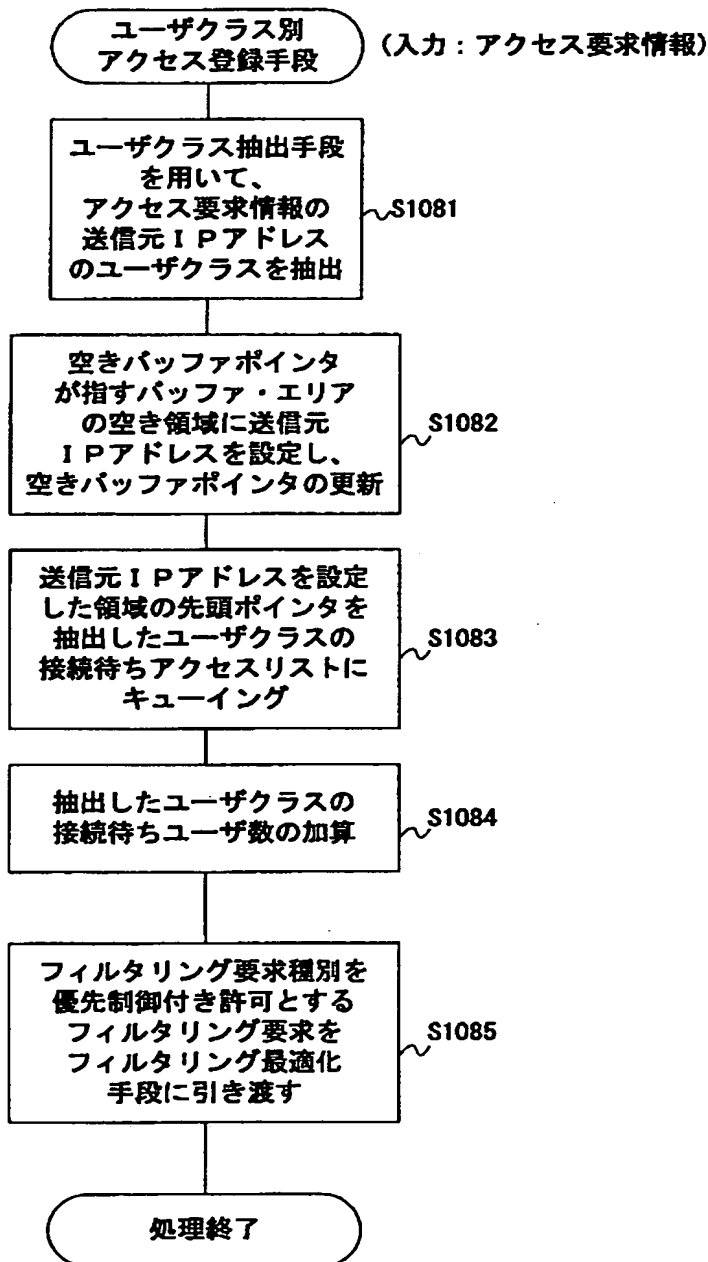
【図 3 3】

動的アクセス許容数算出手段207の処理を  
詳細に説明するためのフローチャート



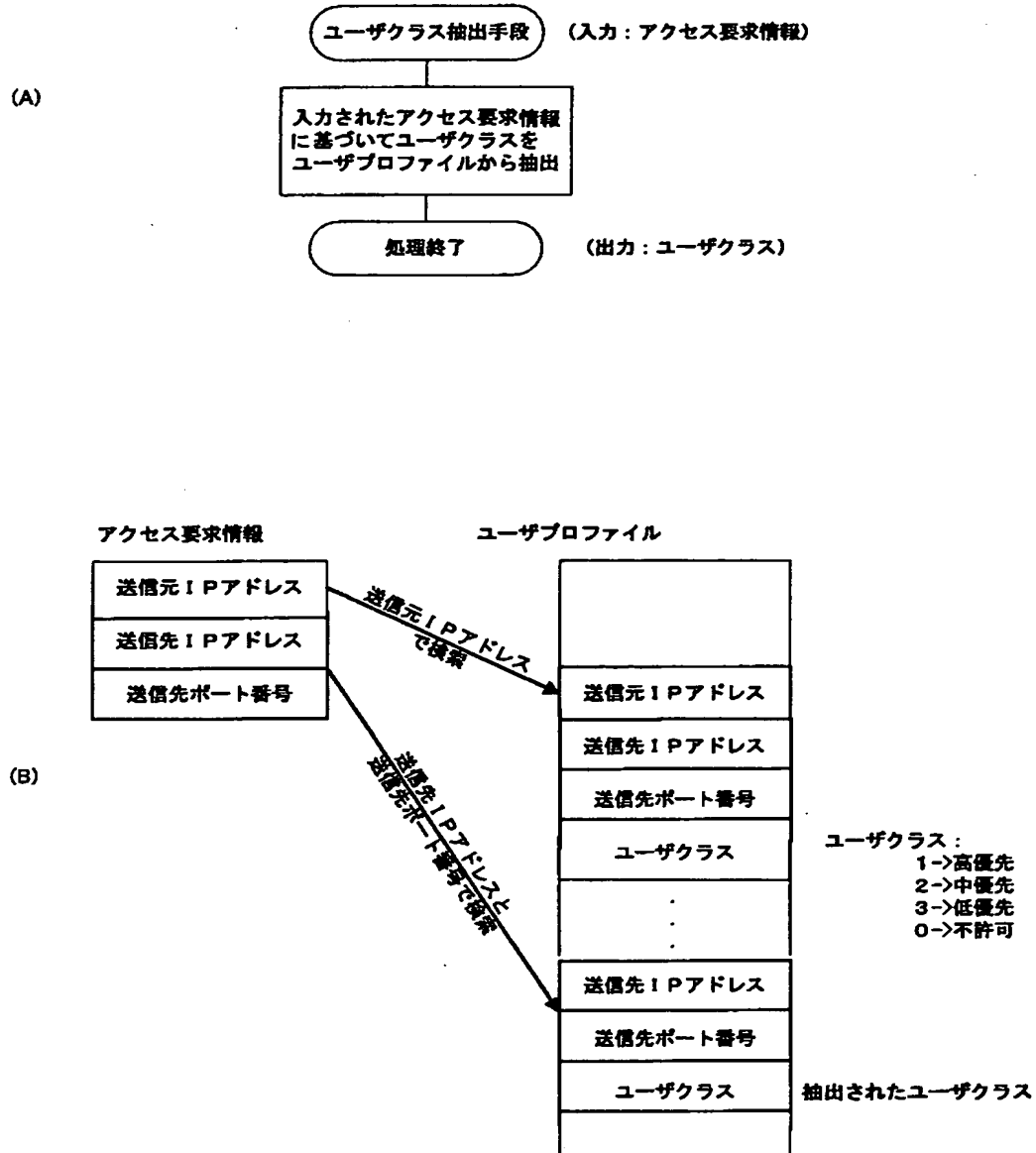
【図 3 4】

ユーザクラス別アクセス登録手段108の処理を  
詳細に説明するためのフローチャート



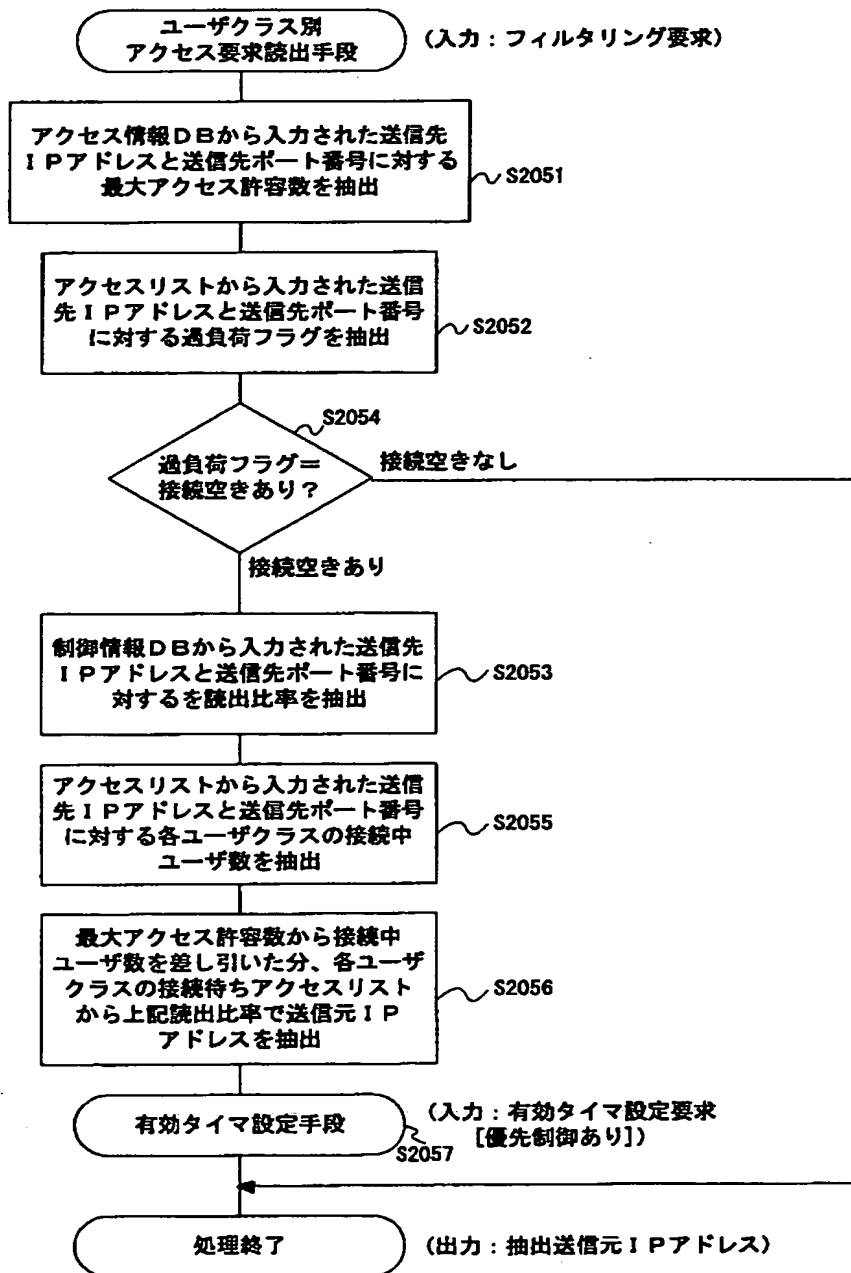
【図 3 5】

ユーザクラス抽出手段102の処理を詳細に説明する図



【図 3 6】

ユーザクラス別アクセス要求読出手段205の処理を  
詳細に説明するためのフローチャート



【図 3 7】

有効タイム設定要求のメッセージ構造を示す図

有効タイム設定要求

要求種別
最大アクセス許容数と 接続中ユーザ数との差分
.
.
最大アクセス許容数と 接続中ユーザ数との差分
送信先 IP アドレス
送信先ポート番号

要求種別：

優先制御あり→0

優先制御なし→1

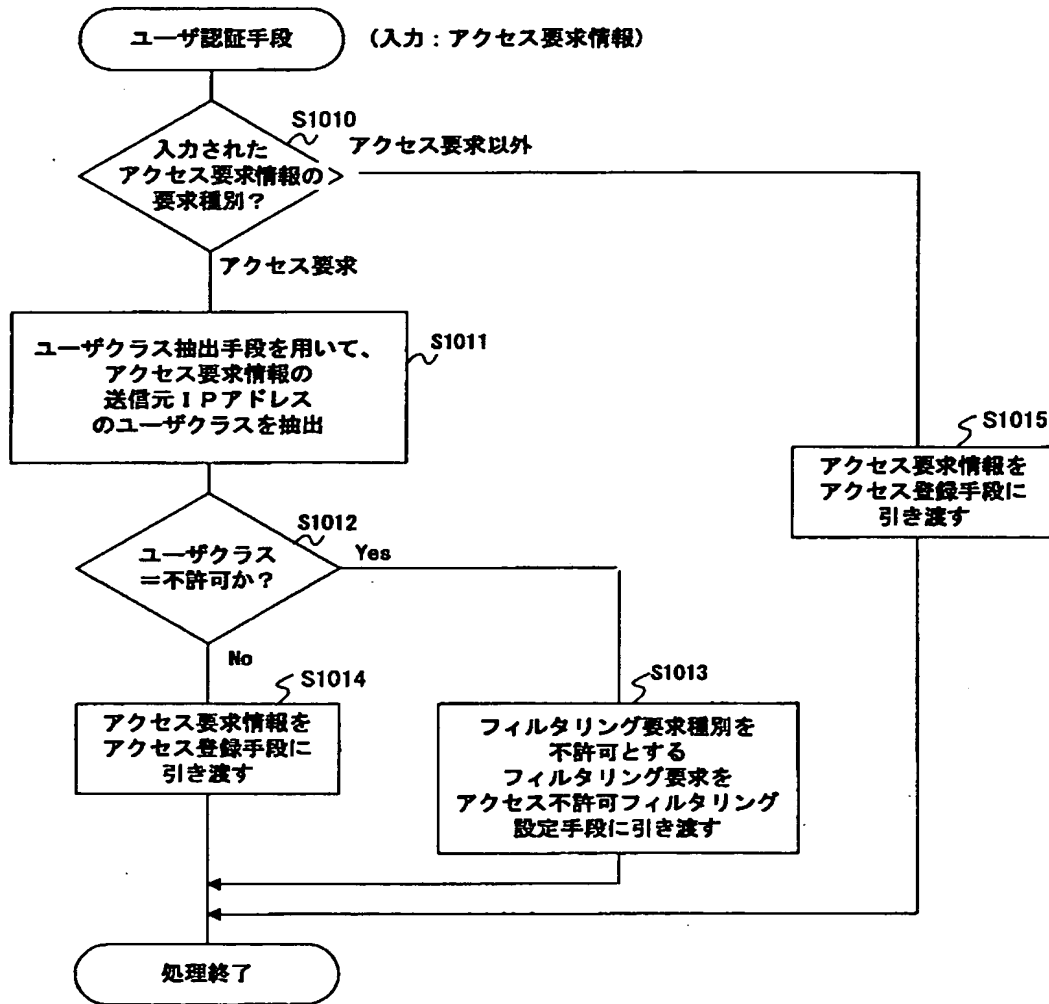
最大アクセス許容数と接続中ユーザ数との差分：

優先制御なしの場合は、データは一つ設定

優先制御ありの場合は、ユーザクラス分設定

【図 3 8】

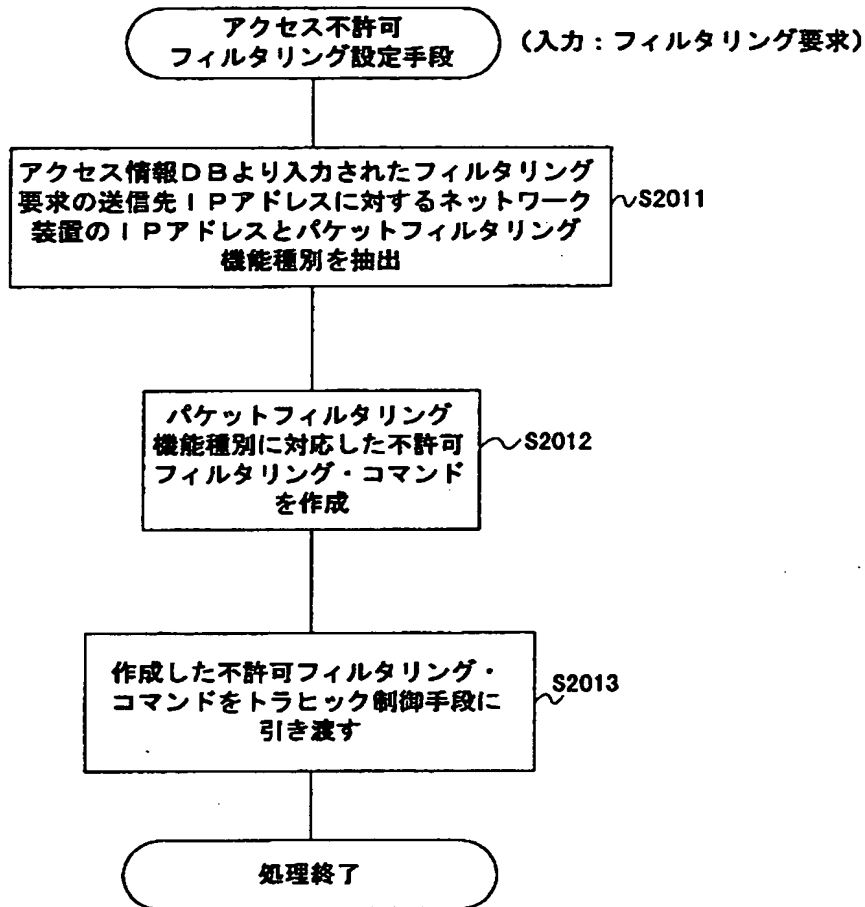
ユーザ認証手段101の処理を詳細に説明するためのフローチャート





【図 39】

アクセス不許可フィルタリング設定手段201の処理を  
詳細に説明するためのフローチャート



【書類名】 要約書

【要約】

【課題】 本発明は、動的オブジェクトを再利用でき、トラヒックの軽減を図ることができ、ユーザに与える負担を軽減でき、アクセス要求したユーザは自分のアクセス順番になれば速い応答速度で快適にサービスを受けることが可能となるネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置を提供することを目的とする。

【解決手段】 受付サーバ100は、ユーザ端末50からのアクセス要求情報を受信して保持し、アクセス制御サーバ200は、サービスサーバ300の処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけアクセス登録手段103に保持されたアクセス要求情報を抽出して前記サービスサーバ300へのアクセスを許容するトラヒック制御を行うため、ユーザがサービスサーバにアクセスする場合に、サービスサーバ300の処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社